ITHOTHO (PTY) LTD

(Registration Number: 2006/005935/07)

POPI Act Policy and PAIA Manual

Version 1 – June 2025

Approved by the Board of Directors on 30 June 2025

INDEX

POPI Act Policy

COMPLIANCE FRAMEWORK AND POLICY IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 OF ITHOTHO (PTY) LTD / ("the COMPANY")

A. INTRODUCTION

1. The objectives of Ithotho (Pty) Ltd, amongst others, is to –

1.1 Conduct business as a totalisator licensee; and

1.2 Ithotho (Pty) Ltd is licensed by the KZNERA.

2. **Definitions**

2.1 In this document the following definitions as it reflects in Section 1 of the Protection of Personal Information Act 4 of 2013 ("POPIA") shall be used where direct reference to the provisions and/or requirements of the POPIA is made or where context necessitates the use of definitions in terms of the POPIA, namely:

2.1.1 **'data subject'** means the person to whom personal information relates;

2.1.2 **'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;

2.1.3 **'information officer'** of, or in relation to, a-

2.1.3.1 public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17 or;

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

2.1.4 **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;

2.1.5 **'person'** means a natural person or a juristic person;

2.1.6 **'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;

2.1.6.1 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;
2.1.6.2 information relating to the education or the medical, financial, criminal or employment history of the person;
2.1.6.3 any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
2.1.6.4 the biometric information of the person;
2.1.6.5 the personal opinions, views or preferences of the person;
2.1.6.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
2.1.6.7 the views or opinions of another individual about the person; and;
2.1.6.8 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.

2.1.7 **'private body'** means:

2.1.7.1 a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
2.1.7.2 a partnership which carries or has carried on any trade, business or profession; or
2.1.7.3 any former or existing juristic person, but excludes a public body;

2.1.8 **'processing'** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including

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

2.1.9 **'record'** means any recorded information

2.1.9.1 regardless of form or medium, including any of the following:

2.1.9.1.1 writing on any material;

2.1.9.1.2 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;

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

2.1.9.1.4 book, map, plan, graph or drawing;

2.1.9.1.5 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;

2.1.9.2 in the possession or under the control of a responsible party;

2.1.9.3 whether or not it was created by a responsible party; and

2.1.9.4 regardless of when it came into existence.

2.1.10 **'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.

2.1.11 **'special personal information'** means the personal information listed in section 26 of the POPIA and includes:

2.1.11.1 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

2.1.12.2 the criminal behaviour of a data subject to the extent that such information relates to-

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

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

2.1.12 **'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**.**

2.2 For ease of reference, certain specific definitions, other than the definitions found in the POPIA, alternatively, definitions adapted from the POPIA's definitions, are listed below as they apply to Ithotho (Pty) Ltd, namely:

2.2.1 **'Biometric Information'** for purposes of Ithotho (Pty) Ltd, and where specifically used in the context of entry to or access to Ithotho (Pty) Ltd, means a technique of personal identification that is based on digitally capturing fingerprints;

2.2.2 **'External Data Subject'** means a data-subject which is not an Internal Data Subject, which includes visitors and employees and representatives of temporary contractors and service providers, who gain access to Ithotho (Pty) Ltd;

2.2.3 **'Internal Data Subject'** means a data-subject in relation to Ithotho (Pty) Ltd which falls into one of the following categories, namely:

2.2.3.1 A Director of Ithotho (Pty) Ltd;
2.2.3.2 An employee of Ithotho (Pty) Ltd;
2.2.3.3 An employee of a contractor or service provider, employed on a basis that such employee regularly gains access to Ithotho (Pty) Ltd.

2.2.4 **'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:

2.2.4.1 any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
2.2.4.2 the Biometric Information of the person;
2.2.4.3 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
2.2.4.4 the views or opinions of another individual about the person; and
2.2.4.5 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.

3. <u>Duty to comply with the POPIA</u>

3.1 Ithotho (Pty) Ltd is a company that must keep certain records in terms of the Companies Act 71 of 2008 ("the Companies Act") and may process other information during its day-to-day administration and management, which includes personal information and, as such, Ithotho (Pty) Ltd is a responsible party as defined in the POPIA.

3.2 Ithotho (Pty) Ltd is committed to comply with the provisions of the POPIA insofar as it relates or pertains to its operations.

3.3 Up to date versions of this policy shall at all times be available on Ithotho (Pty) Ltd's website at www.ithotho.co.za.

3.4 **Details of the Information Officer**

3.4.1 **Full name** – Obayd Naidoo

3.4.2 **Designation** – IT Operations Manager

3.4.3 **Contact details**

3.4.3.1 Physical office address: Suite B10, Rocket Towers, 290 Lenny Naidu Drive, Bayview, Chatsworth, 4092, Kwa-Zulu- Natal
3.4.3.2 E-mail address: paia@sportpesa.co.za
3.4.3.3 Telephone: 021 4863000

3.4.4 The Information Officer is the person described in the PAIA as the head of the company and who must be appointed in terms of the POPIA. Her duties and responsibilities include:

3.4.4.1 Ensuring compliance with the POPIA;
3.4.4.2 Dealing with requests made to the Company in terms of the POPIA;
3.4.4.3 Assisting the Regulator in investigations where the Act requires same;
3.4.4.4 As may further be prescribed in section 55 of the POPIA and the regulations promulgated thereunder.

3.4.5 In the case of Ithotho (Pty) Ltd the Information Officer will be the IT Operations Manager of the company.

3.4.6 Duties of information officers of a company shall specifically include the following:

3.4.6.1 To make sure that the company's POPIA policy is updated and readily available for inspection;
3.4.6.2 To ensure that authorisation is obtained from the Regulator where the Act requires (applicable to processing of unique identifiers for purposes other than the purpose for which it was collected – for instance processing of biometrics used for access control to assist in a criminal investigation).

5.4.7 The Information Officer of the Company is registered with the Information Regulator.

B. THE OUTCOME OF THE PERSONAL INFORMATION IMPACT ASSESSMENT OF THE COMMUNITY SCHEME

1. In terms of regulation 4 of the regulations promulgated under the POPIA, the Information Officer must cause a personal information impact assessment to be executed on behalf of the company, the purpose of which is to ensure that adequate measures and standards are in place in order to comply with the conditions of the lawful processing of personal information as provided for in the POPIA.

2. As a function of the company, the following information may be processed in the normal course of the management and administration of the Company:

2.1 Details of Internal Data Subjects, which details include names, surnames, identity numbers, contact details, and property information of such persons;

2.2 Details of External Data Subjects, which includes names, surnames, identity numbers, contact details, driver's license and vehicle details in relation to such External Data Subject.

3. In exercising its powers and functions, the Company furthermore contracts with third parties ("Operators") who may receive access to and process Personal Information of the aforesaid Internal and External Data Subjects. In this regard, the Company shall enter into an agreement with or request a warranty from such Operators, in substantially the same form as annexure "A" to this framework, in order to safeguard the Company and other data-subjects.

4. **Operators applicable to the Company who may gain access to Personal Information are listed below**

4.1 Security and guarding services

4.1.1 The Personal Information which the Operator has access to are names, surnames, identity numbers, contact details, driver's license, vehicle license and property information which relates to both Internal and External Data Subjects;

4.1.2 The Company shall obtain confirmation of the Operator's POPIA compliance and shall ensure access to the Operator's POPI policy and, where necessary, enter into an agreement with this Operator to ensure that Personal Information remains protected;

4.1.3 For any period that the Company is not in possession of confirmation of the Operator's POPIA compliance or the Operator's POPI policy, the Company shall obtain a compliance guarantee and indemnity from the Operator;

4.1.4 As and when the company renews service agreements with the Operator care shall be taken by the company to ensure that a condition of such service agreements includes a stipulation that the Operator must be POPIA compliant;

4.1.5 The Operator is in possession of this policy document.

C. PROTECTION OF PERSONAL INFORMATION

1. Information to be processed, kept and preserved by the Company

1.1 The Company clearly defines what personal information and documents constitutes, communicates, and assigns accountability for its privacy policy and procedures within its operational structure. As a Responsible Party it has a Monitoring System which monitors compliance with its Policy. Management has procedures in place to address privacy-related complaints disputes and transgressions.

1.2 The Monitoring System provides for the protection, insertion, amendment, and deletion of Personal Information as elected by the relevant data-subject from time to time. This is founded on the following management principles:

1.2.1 Notice

The Company provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed as per the **Consent for Processing Personal Information** available on the website of the company (www.ithotho.co.za).

1.2.2 Choice and Consent

The company describes the choices available to an Internal Data Subject and obtains implicit or explicit consent with respect to the processing of Personal Information.

1.2.3 Collection

The company collects Personal Information only for the purposes of achieving its objectives in terms of its Memorandum of Incorporation and Rules, in terms of prescribed legislation, or as identified in the Consent Form for day to day management of the company.

1.2.4 Use and Retention

The company limits the use of Personal Information to the purposes identified in 1.2.3 above and retains the information for only as long as necessary to fulfil the stated purposes.

1.2.5 Access

The company provides Internal Data Subjects with convenient access to their Personal Information for review and updates, with secure measures in place to avoid unauthorised access by third parties.

1.2.6 Disclosure (to third parties)

The company discloses Personal Information to third parties only for the purposes identified in 1.2.3 above, or with the implicit or explicit consent of the Internal Data Subject.

1.2.7 Security (for privacy)

The company protects Personal Information against unauthorised access (both physical and digital).

1.2.8 Quality

The company maintains accurate, complete and relevant Personal Information for the purposes identified in the Consent for Processing Personal Information.

1.3 In terms of the Companies Act, the company must process the following information and/or documentation

1.3.1 Records of the current directors of the company, including full names, identity number, occupation, date of most recent election or appointment as director and such further information as required in terms of the Act;

1.3.2 Records of past directors as described in paragraph 1.3.1. above for a period of seven years;

1.3.3 Copies of reports presented at general meetings of the company for a period of seven years;

1.3.4 Notices and minutes of all Shareholders' meetings, including resolutions taken by shareholders and documents made available to the shareholders in respect of such a resolution – for a period of seven years;

1.3.5 Copies of written communication sent by the Company to its shareholders generally for a period of seven years;

1.3.6 An updated shareholders' register;

1.3.7 Minutes and resolutions of every directors' meeting, directors' committees' meeting, audit committee meetings for a period of seven years.

1.4 **In terms of the day-to-day administration of the company, the company may process the following Personal Information**

Information relating to access control for security purposes and information required for general and specific communication to shareholders, including:

1.4.1 Personal information of Internal Data Subjects, which include names, surnames, identity numbers, contact details, and property information of such Internal Data Subjects;

1.4.2 Personal information of Internal Data Subjects, which includes names, surnames, identity numbers, contact details, driver's license and vehicle details of such Internal Data Subjects;

2. The Company shall process Personal Information in the ordinary course and scope of its functions, which includes maintaining security and conducting other affairs to the benefit of its shareholders. The Company and its employees shall primarily use Personal Information only for the purpose for which it was originally or primarily collected. Personal Information shall be utilised for a secondary purpose only if such purpose constitutes a legitimate interest and is closely related to the original or primary purpose for which it was collected.

3. **Limitation on information processed and the "minimum information" rule**

3.1 The Company shall record the minimum possible Personal Information of External Data Subjects in order to comply with its security enforcement obligations, but to simultaneously balance the rights of Internal Data Subjects.

3.2 The Company must furthermore process the minimum amount of Personal Information of Internal Data Subjects to comply with the Companies Act and to conduct the day-to-day management and administration of the Company for the benefit of all shareholders.

4. **Responsible processing of Personal Information**

4.1 Personal Information may only be processed by the Company in the following circumstances:

4.1.1 Where the data-subject, or a competent person where the data-subject is a child, consents to the processing;

4.1.2 Where the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data-subject is party;
4.1.3 Where the processing complies with an obligation imposed by law on the responsible party;
4.1.4 Where the processing protects a legitimate interest of the data-subject;
4.1.5 Where the processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the Personal Information is supplied.

4.2 The company, in the course of its day-to-day business, specifically processes Personal Information of Internal Data Subjects, including but not limited to communication with its shareholders or employees via electronic mail, WhatsApp and SMS.

4.3 The company shall ensure that the Personal Information of Internal Data Subjects (including e-mail addresses, contact details and levy account details) are protected.

4.4 Care shall be taken when communication is sent to data-subjects to ensure that Personal Information does not land in the hands of unintended recipients. In this regard:

4.4.1 e-mail addresses of Internal Data Subjects should not be visible in general communication to all Internal Data Subjects; and
4.4.2 e-mails of persons should not be forwarded to third parties without consent from the author thereof or without any other lawful purpose.

4.5 The Company shall not utilize any unique identifier of a data-subject for a purpose other than the purpose specifically intended at collection.

4.6 The Company will consider amendment of its rules from time-to-time in order to protect Personal Information (i.e. steps to be taken by Members who are unintended recipients of communication or who obtains access to personal information by accident or other unlawful manner).

5. **Storage of personal information and security of information**

5.1 All Personal Information shall at all times be kept secured by the company.

5.2 In the case of hard copy documents, such documents shall be stored in a lockable cabinet, a safe room or safe, depending on its nature.

5.3 Only authorised persons, which includes the Information Officer and persons authorised by the Information Officer, shall have limited access to such personal information.

5.4 In the case of digital data locally stored, such data containing personal information shall be stored on a computer that requires a password for access. Data backups of the

computer in question shall take place via storage of such backup data on a password protected flash drive. Insofar these passwords are concerned, only the Information Officer and his authorised personnel have the passwords.

5.5 In the case of digital data in the cyber space, such data containing personal information shall be stored with a POPIA compliant operator in the cloud, which is only accessible by password which the Information Officer and his authorised personnel has.

6. Information processed which should be destroyed as soon as possible after its purpose was served

6.1 Any Personal Information processed and stored by the company in terms of statute must only be kept for as long as required by such statute unless longer storage can be motivated.

6.2 The company is under no obligation in law to keep the access control information for Internal and External Data Subjects for extensive periods.

6.3 Any of the aforesaid access control information which is not required by law to be kept on record for a fixed period shall be destroyed by the responsible party as soon as it has served the purpose for which it was processed. In this regard, the company shall retain any personal information which is processed for a specific administration purpose (such as security and access control) only for as long as same may serve a purpose and for no longer than 12 (twelve) months. The reason for this period is that the information may be required for a lawful purpose (e.g. to assist in an investigation by authorities regarding a security breach).

7. Form of destruction or deletion of personal information

7.1 Once Personal Information becomes redundant or is no longer required by law to be stored, the company shall destroy or delete such information.

7.2 In the case of physical documentation, permanent destruction shall be ensured by way of shredding or recycling documents with a POPIA compliant operator.

7.3 In the case of digital information in the cyber space, the relevant data files shall be deleted permanently in a form in which it cannot be directly retrieved by the company.

7.4 The operational system that the company has put in place for the destruction/deletion of personal information is as follows:

7.4.1 The Information Officer shall on a monthly basis peruse the information in possession of the company with the purpose of determining which Personal

Information items are redundant and no longer required by law or in terms of this manual;

7.4.2 Physical documents identified shall be shredded or recycled as provided for in this manual;

7.4.3 Digital information identified shall be permanently deleted from all hard drives and flash drives.

8. Consent to processing of personal information by data subject

8.1 In terms of the company, processing of information is allowed once consent of the data subject is obtained.

8.2 The processing of information must still be for a lawful purpose or for a legitimate objective and may relate to specific Personal Information.

8.3 The company provides a **Consent for Processing Personal Information** form on its website (www.ithotho.co.za).

9. Data breaches – what to do in case personal information is leaked

9.1 The company is committed to protecting Personal Information and to avoid data breaches.

9.2 Should a data breach be committed by an Operator, the company shall engage the Operator to mitigate the breach and investigate the origin of the breach.

9.3 If the origin of the breach is with the Operator, the company shall request the Operator to report the breach to the Information Regulator. If it refuses, the company may report the breach of information to the Information Regulator if it relates to any closely related person to it, for instance its Members and Residents.

9.4 If the breach originated as a result of an act or omission on the part of the company, the Information Officer shall immediately report the breach to the Information Regulator, shall investigate the breach and without delay prepare a report based on his findings.

10. Training

10.1 The company shall train its representatives and staff on a continual basis as necessary, but at this stage at least yearly, regarding compliance with the processing of information and destruction of unnecessary and redundant information.

10.2 Operators shall be vetted by the company (and through its employees or contractors appointed for such purpose, where applicable) to ensure compliance with the POPIA by said Operators such as service providers of the company;

10.3 Training feedback questionaries shall be completed by all participants of the training provided by the company in order to actively monitor and control the protection of Personal Information.

10.4 The company shall furthermore utilize any training feedback in order to adapt, update and improve this manual every 12 (twelve) months.

11. **Continual development of policy**

The company acknowledges that assessment of its compliance must be conducted regularly (at this stage, at least yearly) and that this policy should be adapted as and when required. It is the responsibility of the relevant interested party or data-subject to ensure that the latest version of this policy is obtained from the company's website.

D. THE PROMOTION OF ACCESS OF INFORMATION ACT 2 OF 2000 (PAIA) AND ACCESS TO INFORMATION IN TERMS OF THE COMPANIES ACT

1. Any person may request information held by the company in terms of the PAIA. Shareholders may, in addition to the PAIA, also request specified records or information in terms of section 26 of the Companies Act.

2. Persons other than Shareholders of the company may request copies of the Shareholders' register held by the company and the Directors' register in terms of section 26 of the Companies Act.

3. Persons other than Shareholders may request information in terms of the PAIA.

4. Requests for access to information in terms of the PAIA is dealt with in the company's PAIA manual, including:

4.1 The format of the request and requirements to be met before information shall be released;

4.2 Timelines for processing information pursuant to a request in terms of PAIA as well as the decision to make information available.

4.3 The form in which information is to be made available;

4.4 Recovery of costs of information processing and dispatch in terms of PAIA;

4.5 POPI Act Reference guide.

5. Data-subjects may, in terms of section 23 of the POPIA, request access to their Personal Information held by the Company and may, in terms of section 24, challenge its correctness or request that the Personal Information be deleted or destroyed.

E. DOCUMENTS ANNEXED TO THIS POLICY

1. An example of an **operator compliance guarantee** is annexed hereto marked as **Annexure A.**

2. A **quick reference guide on the processing of personal information**, the retention and storage thereof as well as the destruction of information is annexed to the policy as **Annexure B**. This reference guide is ideal to assist employees of the Company to understand the purpose of the POPIA and to comply with its provisions.

ANNEXURE "A"

GUARANTEE IN RESPECT OF COMPLIANCE

With the Protection of Personal Information Act 4 of 2013 ("POPI Act")

BY: OPERATORS COMPANY NAME:
("the OPERATOR")
REGISTRATION NUMBER:
AUTHORISED RESPRESENTATIVE:
IN FAVOUR OF: ITHOTHO (PTY) LTD REGISTRATION NO:
("the RESPONSIBLE PARTY")

I, the undersigned _____ in my capacity as _____ duly authorised representative on behalf of _____ ("the Operator") hereby declare that the Operator is POPI Act compliant and that any personal information which is processed in the course of the Operator's functions and services rendered to Ithotho (Pty) Ltd ("the Responsible Party") shall be processed in accordance with the POPI Act.

The Operator hereby indemnifies and holds harmless the Responsible party against any claims by any third party who alleges personal information breaches and/or irresponsible processing of personal information and/or any action or omission which may, if proven, lead to an offence being committed in terms of the POPI Act, where such personal information was not adequately protected in terms of the POPI Act due to an act or omission on the Operator's part.

I further declare that I am the information officer, alternatively the duly appointed agent of the Operator and I am duly authorised on behalf of the Operator to execute this compliance declaration.

I acknowledge and understand that I may incur personal liability in terms of the penalties applicable for committing an offence under the POPI Act should I sign this document without authority of the Operator or if this warrantee is breached.

Dated and signed at _____ on this the _____ day of _____

Full names and surname: _____
Identity number: _____
Contact details: _____
Physical Address: _____
_____
_____

_____ obo the Operator who warrants his authority to do so

ANNEXURE "B" QUICK REFERENCE GUIDE

on the Protection of Personal Information Act 4 of 2013 ("the POPI Act")

1. The POPI Act came into operation on the 30 June 2021. After this date all responsible parties need to comply with the Act.

2. The purpose of the POPI Act is to promote protection of personal information which information is processed by public and/or private bodies. A Company, such as Ithotho (Pty) Ltd is a private body.

3. The Act prescribes certain requirements for the processing of personal information to ensure that such processing is reasonable, and that personal information is adequately protected.

4. Personal information has a wide meaning, and the Act defines personal information as follows:

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

- 4.1.1 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;
- 4.1.2 information relating to the education or the medical, financial, criminal or employment history of the person;
- 4.1.3 any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
- 4.1.4 the biometric information of the person;
- 4.1.5 the personal opinions, views or preferences of the person;
- 4.1.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- 4.1.7 the views or opinions of another individual about the person; and
- 4.1.8 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

4.2 Other definitions which are important to note for purposes of this guide are as follows:

- 4.2.1 **Data-subject**: Is the person to whom personal information relates.

4.2.2 **Information officer**:

4.2.2.1 public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or;
4.2.2.2 private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act.

4.2.3 **Processing**: Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including

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

4.2.4 **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.

5. Viewed practically, the following basic principles apply when personal information of data-subjects is processed:

5.1 The minimum amount of information to serve the purpose thereof must be collected;

5.2 The information must be kept in a safe place to which access is limited to the Information Officer or the data collector authorised by the Information Officer – to avoid intentional and/or unintentional/accidental disclosure to third parties;

5.3 Personal information which was processed and stored must only be kept for as long as it may be necessary in terms of the purpose for which it was collected and as soon as it does not serve a purpose or is not required to be stored, it must be destroyed.

6. When personal information is processed (i.e. handled, collected etc.), individual data-subjects' information must not be visible to other data-subjects.

7. If personal information is processed, it should be stored in a safe place where third parties do not have access to said personal information.

8. If personal information was stored after processing, it must be destroyed as soon as it has served its purpose, for example:

8.1 When an entry log is signed to gain access to the property of a private and/or public body, the minimum information must be collected to comply with security protocol, the information must only be stored for a minimum amount of time in order to comply with security protocol (i.e. no more than a month or two, depending on the necessity of record-keeping and the purpose for which the information is collected), the information collected must not be divulged to any other party than the relevant data subject from which it is collected or processed and, finally, the personal information must be destroyed in a manner so that it is not retrievable after destruction (i.e. shredding, deletion or destruction by the private body, alternatively, recycling, destruction or deletion by a responsible third party operator which is POPI Act compliant).

8.2 Where information of a data-subject is processed and it required to be stored or extensive periods of time in terms of statute, it must be stored in a safe place which is not accessible to third parties and after the prescribed statutory period, it must be destroyed in an irretrievable manner (i.e. shredding, deletion or destruction by the private body, alternatively, recycling, destruction or deletion by a responsible third party operator which is POPI Act compliant).

9. The general rule of thumb when working with personal information of a data-subject is as follows:

9.1 Only record necessary information to serve the purpose for which it is processed (i.e. scanning of driver's licence and licence disk to gain access to the scheme for security purposes, temperature readings taken for compliance with the Disaster Management Act regulations applicable from time to time);

9.2 Don't store the information if it will serve no purpose or if it is not prescribed by legislation;

9.3 Destroy information as soon as possible after it had become redundant (i.e. where it becomes unnecessary to keep or when prescribed periods for record keeping elapses);

9.4 Never give out any personal information collected to third parties;

9.5 When in doubt, contact your Information Officer for directions relating to personal information which you have processed and/or are about to process in the course and scope of your employment or other contract.

PAIA MANUAL

MANUAL IN TERMS OF SECTION 51 OF THE
PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000 ("PAIA") OF ITHOTHO (PTY) LTD
("the COMPANY")

1. IMPORTANT DEFINITIONS CONTAINED IN THE PAIA

1.1 **'Head'** of, or in relation to, a private body means

1.1.1 in the case of a natural person, including a person referred to in paragraph (c) of the definition of 'political party', that natural person or any person duly authorised by that natural person;
1.1.2 in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
1.1.3 in the case of a juristic person:

1.1.3.1 the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or
1.1.3.2 the person who is acting as such or any person duly authorised by such acting person; or
1.1.4 in the case of political party, the leader of the political party or any person duly authorised by that leader;

1.2 **'Person'** means a natural person or a juristic person.

1.3 **Personal requester'** means a requester seeking access to a record containing personal information about the requester;

1.4 **'Private body'** means -

1.4.1 a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
1.4.2 a partnership which carries or has carried on any trade, business or profession;
1.4.3 any former or existing juristic person; or
1.4.4 a political party,

but excludes a public body.

1.5 **'Record'** of, or in relation to, a public or private body, means any recorded information

1.5.1 regardless of form or medium;
1.5.2 in the possession or under the control of that public or private body, respectively; and
1.5.3 whether or not it was created by that public or private body, respectively;

1.6 **'Request for access'**, in relation to

1.6.1 a public body, means a request for access to a record of a public body in terms of section 11; or
1.6.2 a private body, means a request for access to a record of a private body in terms of section 50;

1.7 **'Requester'**, in relation to:

1.7.1 a public body, means

1.7.1.1 any person (other than a public body contemplated in paragraph (a) or (b) (i) of the definition of 'public body', or an official thereof) making a request for access to a record of that public body; or
1.7.1.2 a person acting on behalf of the person referred to in subparagraph 1.7.1.1;

1.7.2 a private body, means

1.7.2.1 any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body; or
1.7.2.2 a person acting on behalf of the person contemplated in subparagraph 1.7.2.1;

2 INTRODUCTION AND DESCRIPTION OF THE PRIVATE BODY

2.1 The objective of Ithotho (Pty) Ltd, amongst others, is to conducts business as a bookmaker and is licensed by the Western Cape Gambling and Racing Board.

2.2 The company is regulated by the Companies Act 71 of 2008, the Memorandum of Incorporation of the company and rules created in terms of the aforesaid.

3 CONTACT DETAILS OF THE INFORMATION OFFICER

3.1 The information officer of the company shall be deemed to be IT Operations Manager of the company who is in office from time-to-time.

3.2 The details of the information officer of the company are as follows:

3.2.1 **Full name** – Obayd Naidoo

3.2.2 **Contact details**

3.2.2.1 Physical office address: Suite B10, Rocket Towers, 290 Lenny Naidu Drive, Bayview, Chatsworth, 4092, Kwa-Zulu Natal
3.2.2.2 E-mail address: paia@sportpesa.co.za
3.2.2.3 Telephone: 0214863000

The Human Rights Commission, in terms of Section 10 of PAIA, issued a guide on how to use the PAIA, which is published in several languages and available at www.sahrc.org.za.

4 SUBJECTS ON WHICH RECORDS ARE HELD BY THE COMPANY

4.1 **The company holds records of information on the following subjects and for the following periods**

4.1.1 **In terms of section 24 of the Companies Act, the company must keep records of following information and/or documentation**

4.1.1.1 Records of the current directors of the company, including full names, identity number, occupation, date of most recent election or appointment as director and such further information as required in terms of the Act;
4.1.1.2 Records of past directors as described in (a) above for a period of seven years;
4.1.1.3 Copies of reports presented at general meetings of the company for a period of seven years;
4.1.1.4 Notices and minutes of all shareholders' meetings, including resolutions taken by shareholders and documents made available to the shareholders in respect of such a resolution – for a period of seven years;

4.1.1.5 Copies of written communication sent by the company to its shareholders generally for a period of seven years;
4.1.1.6 An updated Members' register;
4.1.1.7 Minutes and resolutions of every directors' meeting, directors' committees' meeting, audit committee meetings for a period of seven years.

4.1.2 **Personal information collected from data subjects which is protected by the Protection of Personal Information Act (POPIA):**

Information relating to access control into the company, including:

4.1.2.1 Names, identity numbers, contact details and designations of visitors, employees and contractors.

4.2 **The right to request information in terms of the Companies Act Section 26**

4.2.1 In terms of Section 26 of the Companies Act 71 of 2008 a shareholder may request the information mentioned in section 24 of the Companies Act.
4.2.2 A shareholder's right to request information in terms of PAIA is not limited by the provisions of the Companies Act.
4.2.3 A non-member may request the following information of the company:

4.2.3.1 Persons other than shareholders may request copies of the shareholders' register held by the company and the Directors' register in terms of section 26 of the Companies Act.
4.2.3.2 Persons other than shareholders may request any additional information relating to the company in terms of the PAIA and in terms of this manual.

5 REQUEST FOR ACCESS TO RECORDS OF THE COMPANY

5.1 Any interested party who wishes to obtain access to a records of the company shall apply for access to such a record as indicated herein below**:**

5.1.1 Any record may be requested by making use of the following process:

5.1.1.1 All records may be requested from the head in writing and in compliance with the PAIA and this manual;
5.1.1.2 The company shall not make available any information for inspection and shall only, after considering a request for access to information, provide copies thereof to the requester (electronically or otherwise). Only in exceptional circumstances, where it is impossible to provide copies, will inspection be arranged.

5.1.1.3 The company shall be entitled to demand payment of a request fee and access fee as determined in terms of item 2, part 3 of the regulations promulgated under the PAIA. The aforesaid request and access fees are attached hereto marked as annexure "**A"**.

5.1.1.4 A request referred to above shall be in writing, substantially in the form of the attached prescribed **Form C** attached as annexure "**B**" to this document, and stating / complying with the following additional requirements:

5.1.1.4.1 A request shall be delivered via e-mail for the attention of the Information Officer of the company to the address as provided for in this manual;

5.1.1.4.2 The full names, physical address and identity number of the requester;

5.1.1.4.3 Indicating whether the requester is a shareholder or not, alternatively, whether the application is made on behalf of another party. In such case the other party and the capacity in which the request if made on behalf of the other party needs to be stated;

5.1.1.4.4 Indicating the number of the unit/erf which the requester owns if the requestor is a shareholder;

5.1.1.4.5 If the requester is not a shareholder, he/she/it shall state its capacity (i.e. visitor, employee or contractor of the company or of a shareholder).

5.1.1.4.6 If the request for information is made on behalf of another person, the requester must provide authorisation for such a request and furnish proof of his/her/its capacity in relation to the person on whose behalf the request is made;

5.1.1.4.7 Specifying the type of document or information requested (the subject and category within which the document or information falls);

5.1.1.4.8 specification of the date/year of the document if the document is produced periodically or where more than one version of the document is likely to exist;

5.1.1.4.9 indicate which right the requester seeks to protect or exercise with the information requested and provide an explanation why the requested document or information is necessary to protect or exercise his/her/it's right;

5.1.1.4.10 Indicate why the record is requested in terms of PAIA and not in terms of the Companies Act;

5.1.1.4.11 Indicate whether an electronic or hard copy of document is requested and, if an electronic document is requested (and where it is possible to furnish same electronically) an e-mail address for delivery thereof should be provided;

5.1.1.4.12 written replies to the request shall be furnished by way of electronic mail, unless indicated otherwise by the requester.

5.1.2 Once the company is in receipt of a request for information, it shall acknowledge the request within 7 (seven) business days, unless otherwise communicated.

5.1.3 The request shall thereafter be referred to the head of the company for consideration and a response.

5.1.4 Once the request is approved, an invoice shall be sent to the requester for payment of the request fee and access fee.

5.1.5 If the request is denied, the requester shall be informed within 30 (thirty) days, subject to extension as provided for in the PAIA.

5.1.6 The company shall not make available any personal information to a requester/personal requested without strict compliance with the POPI Act, as read with the PAIA.

5.1.7 In terms of section 51(2) of PAIA, this manual must be updated on a regular basis and it is the duty of requesters to conform to the process described in the latest available version of the manual.

ANNEXURE "A"

Request fees and access fees applicable to a request in terms of PAIA

Fees in respect of private bodies

1. The fee for a copy of the manual as contemplated in regulation 9(2)(c) is R1.10 for every photocopy of an A4 size page or part thereof.

2. The fees for reproduction referred to in regulation 11(1) are as follows:

a)	For every photocopy of an A4 size page or part thereof	R1.10.
b)	For every printed copy of an A4size page or part thereof held on a computer or in electronic or machine-readable form	R0.75
c)	For a copy in a computer readable form on: (i) USB (ii) External hard-drive	 R7.50 R70.00
d)	(i) For a transcription of visual images, for an A4-size page or part thereof (ii) For a copy of visual images	R40.00 R60.00
e)	(iii) For a transcription of visual images, for an A4-size page or part thereof (iv) For a copy of visual images	R20.00 R30.00

3. The request fee payable by a requester, other than a personal requester, referred to in regulation 11(2) is R50.00.

4. The access fees payable by a requester referred to in regulation 11(3) are as follows:

a)	For every photocopy of an A4-size page or part thereof	R1.10
b)	For every printed copy of an A4size page or part thereof held on a computer or in electronic or machine-readable form	R0.75
c)	For a copy in a computer readable form on: (i) stiffy disc (ii) compact disc	 R7.50 R70.00
d)	(i) For a transcription of visual images, for an A4 size page or part thereof (ii) For a copy of visual images	R40.00

		R60.00
e)	(i) For a transcription of an audio record, for an A4size page or part thereof (ii) For a copy of an audio record	R20.00 R30.00
	To search for and prepare the record for disclosure, R30.00 for each hour or part of an hour reasonably required for such search and preparation	

5. For purposes of section 54(2) of the Act, the following applies:

a)	Six hours as the hours to be exceeded before a deposit is payable; and
b)	one third of the access fee is payable as a deposit by the requester.

6. The actual postage is payable when a copy of a record must be posted to a requester.

ANNEXURE "B"

J752

REPUBLIC OF SOUTH AFRICA

FORM C
REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY
(Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))
[Regulation 10]

A. Particulars of private body
The Head:

B. Particulars of person requesting access to the record

(a) The particulars of the person who requests access to the record must be given below.
(b) The address and/or fax number in the Republic to which the information is to be sent must be given.
(c) Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname: .....

Identity number: | | | | | | | | | | | | | |

Postal address: .....

Telephone number: (.....) ..... Fax number: (.....) .....

E-mail address: .....

Capacity in which request is made, when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname: .....

Identity number: | | | | | | | | | | | | | |

FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

D. Particulars of record

(a)	Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
(b)	If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Description of record or relevant part of the record:

.....

.....

.....

.....

2. Reference number, if available:

.....

.....

.....

.....

3. Any further particulars of record:

.....

.....

.....

.....

E. Fees

(a)	A request for access to a record, other than a record containing personal information about yourself, will be processed only after a request fee has been paid.
(b)	You will be notified of the amount required to be paid as the request fee.
(c)	The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.
(d)	If you qualify for exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

.....

.....

.....

.....

.....

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 below, state your disability and indicate in which form the record is required.

Disability: Form in which record is required:

Mark the appropriate box with an **X**.

NOTES:
(a) Compliance with your request for access in the specified form may depend on the form in which the record is available.
(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
(c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:						
	copy of record*		inspection of record			
2. If record consists of visual images - (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):						
	view the images		copy of the images*		transcription of the images*	
3. If record consists of recorded words or information which can be reproduced in sound:						
	listen to the soundtrack (audio cassette)		transcription of soundtrack* (written or printed document)			
4. If record is held on computer or in an electronic or machine-readable form:						
	printed copy of record*		printed copy of information derived from the record*		copy in computer readable form* (stiffy or compact disc)	

*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES	NO

G. Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form.
The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

……

……

……

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

……

……

……

FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved / denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

……..

Signed at …….. this day…… of ……year …….

……
SIGNATURE OF REQUESTER /
PERSON ON WHOSE BEHALF REQUEST IS MADE