THE GROUP COMPANY POLICY ON THE PROTECTION OF PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA)

For the purposes of this Policy unless otherwise noted, all references to the Institute of Election Management Services (hereinafter referred to as "the Company" or "IEMSA" or "Responsible Party") includes a reference to all the Company subsidiaries and listed third parties.

To view the comprehensive list of the abovementioned parties please make application for access to this listing by following the procedure set out under the Company PAIA Manual accessible by accessing the company website at www.iemsa.co.za.

INDEX

1. INTRODUCTION

The Protection of Personal Information Act, 4 of 2013 (POPIA) regulates and controls the processing of Personal Information.

The Company is a company rendering election management and capacity building services.

The Company, for the purposes of carrying out its business and related objectives, does and will from time to time, processes the Personal Information of living individuals and legal entities including public and private entities, such as Personal Information pertaining to employees and staff, part-time employees and independent contractors, prospective employees and job applicants, students and interns, service providers and contractors, vendors, clients, election electorate and voters, customers, and other third parties.

The Company is obligated to comply with POPIA and the data protection conditions housed under POPIA with respect to the processing of all and any Personal Information.

This Policy describes how the Company will discharge its duties in order to ensure continuing compliance with POPIA in general and the information protection conditions and rights of data subjects in particular.

2. DEFINITIONS

Take note of the following definitions which will be used throughout this Policy and which are used under POPIA.

"biometrics" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
"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 decision in respect of any matter concerning him-or herself;
"competent person" means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;

"consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;
"data subject" means the person to whom Personal Information relates;
"Operator" means a person who processes Personal Information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;
"person" means a natural person or a juristic person;
"Personal Information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
(a)information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b)information relating to the education or the medical, financial, criminal or employment history of the person;
(c)any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d)the biometric information of the person;
(e)the personal opinions, views or preferences of the person;
(f)correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g)the views or opinions of another individual about the person; and
(h)the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person;

Examples of Personal Information include
A person's name and address (postal and email)
Date of birth
Statement of fact
Any expression or opinion communicated about an individual
Minutes of meetings, reports
Voters' rolls
Attendance registers
Emails, file notes, handwritten notes, sticky notes
Photographs and CCTV footage if an individual can be identified by the footage
Employment and student applications
Spreadsheets and/or databases with any list of people set up by code or student/staff
Employment number
Employment or education history
Banking details
Special Personal Information Includes:
Any information relating to an individual's:
Ethnicity
Gender
Religious or other beliefs
Political opinions
Membership of a trade union
Sexual orientation
Medical history
Offences committed or alleged to have been committed by that individual
Biometric details
Children's details

"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;
"public record" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;
"record" means any recorded information—
(a)regardless of form or medium, including any of the following:
(i)Writing on any material;
(ii)information produced, recorded or stored by means of any 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 any thing of which it forms part, or to which it is attached by any means;
(iv)book, map, plan, graph or drawing;
(v)photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
(b)in the possession or under the control of a responsible party;
(c)whether or not it was created by a responsible party; and
(d)regardless of when it came into existence;
"responsible party" means a public or private body or any other person who, alone or in conjunction with others, determines the purpose of and means for processing personal information;

3. PURPOSE AND OBJECTIVES

3.1 This Policy sets out how the Company deals with Personal Information.

3.2 This Policy forms part of the Company's commitment to the safeguarding of Personal Information processed by it and its staff, operators and or service providers.

3.3 The objective and purpose of this Policy is to:

3.3.1 set out the Company's policy on the processing of Personal Information;

3.3.2 ensure that all Company directors, executives, employees, contractors and where applicable Company service providers, clients and Operators process Personal Information in accordance with POPIA and the POPIA conditions for the lawful processing of personal information;

3.3.3 provide a guideline to Company directors, executives, employees, contractors, and where applicable Company service providers, clients and Operators, on how the Company will process Personal Information.

3.4 This Policy is available on the Company website www.iemsa.co.za and on request from the Company Information Officer.

3.5 This Policy is drafted in conjunction with the Company's Privacy statement, the Company Section 18 Informed Consent notice, and POPIA guidelines available on the Company website www.iemsa.co.za and on request from the Company Information Officer.

4. THE DATA PROTECTION PRINCIPLES AND CONDITIONS

4.1 It is the duty of a Responsible Party and the Company to comply with all the data protection conditions set out under section 4 of POPIA, which are as follows:

4.1.1 Personal Information shall be obtained and processed fairly and lawfully.

4.1.2 Personal Information shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes, unless specific consent to do so has been obtained.

4.1.3 Personal Information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4.1.4 Personal Information shall be accurate and, where necessary, kept up to date.

4.1.5 Personal Information processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

4.1.6 Personal Information shall be processed in accordance with the rights of data subjects under POPIA.

4.1.7 Appropriate technical and organisational safeguards and measures must be put in place to protect and guard against unauthorised or unlawful processing of Personal Information and against accidental loss or destruction of, or damage to, personal data.

4.1.8 Personal Information shall not be transferred to another country unless that country or the person transferring the Personal Information ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5. APPLICATION AND SCOPE

5.1 This Policy applies to all Personal Information processed by or on behalf of the Company and to the following persons:

5.1.1 all employees of the Company, who for the purposes of this Policy, means and will include all members of staff including permanent, fixed term, and temporary staff, directors and executives, secondees, any third-party representatives, agency workers, volunteers, interns, agents and sponsors engaged with The Company in South Africa, or overseas.

5.1.2 all employees employed by any of the Company's subsidiary or associated companies.

5.1.3 all Operators, service providers, contractors and agents acting for or on behalf of the Company, provided they have been made aware of this Policy.

6. PERSONAL INFORMATION COLLECTED

6.1 The Company collects and processes Personal Information from a number of persons in order to carry out and pursue its business and related operational interests.

6.2 The type of Personal Information, which the Company processes, will depend on the need for which it is collected and will be processed for that purpose only.

6.4 Examples of Personal Information which the Company will from time to time collect includes but is not limited to:

- the person’s identity number, name, surname, address, postal code, marital status, and how many dependents they have;
- the person’s description of residence, business, assets; financial information, banking details;
- the person’s description of health, biometric details, expertise, qualification and skills;

- any other information required by The Company or its service providers, and suppliers in order to provide an accurate analysis of that person's needs;

- Information on a person's requirements, needs and specifications which is or may be used for marketing purposes to ensure that the Company products, services and offerings remain relevant and applicable;

- further processing, provided it is in line with the provisions of POPIA.

6.5 Any person, be it an employee or a person acting on behalf of the Company will provide each person from whom Personal Information is collected for the purpose of processing, a standard Company section 18 informed consent document, a copy of which is annexed hereto.

7. HOW PERSONAL INFORMATION IS USED

7.1 The Company will only use a person's Personal Information for the purpose for which it was collected and agreed. This may include:

- conducting of elections;

- conducting training and capacity building;

- recruitment and employment purposes;

- conducting criminal reference checks;

- for risk assessments, insurance and underwriting purposes;

- assessing and processing queries, enquiries, complaints, and / or claims;

- conducting credit reference searches or verification;

- confirming, verifying and updating persons details;

- for purposes of personnel and other claims history;

- for the detection and prevention of fraud, crime, money laundering or other malpractice;
- conducting market or customer satisfaction research;
- direct marketing purposes;
- audit and record keeping purposes;
- in connection with legal proceedings;
- providing services to clients to carry out the services requested and to maintain and constantly improve the relationship;
- providing communications in respect of The Company, its employees or other persons to governmental officials and regulatory agencies; and
- in connection with and to comply with legal and regulatory requirements or when it is otherwise required or allowed by law.

8. INFORMED CONSENT

8.1 In accordance with POPIA, the Company, its employees and or Operators, will use its best endeavours, (save where it is unable to and this is due to it protecting the legitimate interests of the person whose Personal Information it is processing or the legitimate interests of the Company itself), only process Personal Information if the below mentioned conditions are met, which conditions are set out in the Company standard section 18 informed consent document, annexed hereto:

8.1.1 the person is told why the processing is necessary, what information is required and what will be done with it;

8.1.2 the person consents to the processing, which consent will be obtained at the time when that person's Personal Information is processed;

8.1.3 the processing is necessary i.e. in order to conduct an accurate analysis of that person's needs for purposes of amongst other employment reasons, credit limits, insurance requirements;

8.1.4 the processing is required as a result of or in order to comply with an obligation imposed by law on the Company;

8.1.5 the processing protects a legitimate interest of the person and it is in the person's best interest to have a full and proper needs analysis performed in order to provide them with an applicable and beneficial product or service;

8.1.6 processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom the Personal Information is supplied.

9. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

9.1 The Company may from time to time have to disclose certain Personal Information, which it has obtained from persons to other parties, including its group companies or subsidiaries, joint venture companies and or approved product or third party service providers, auditors, regulators and or governmental officials, overseas service providers and related companies or agents, but such disclosure will always be subject to an agreement which will be concluded as between the Company the party to who it is disclosing, which contractually obliges the recipient of the Personal Information to comply with strict confidentiality and data security conditions. A copy of this standard type agreement is available on request from the Information Officer.

10. SAFEGUARDING PERSONAL INFORMATION

10.1 All Company employees and where applicable, Operators and persons acting on behalf of the Company must before processing Personal Information ensure that the data will be kept secure and that appropriate measures and safeguards are in place to prevent any unauthorised access, disclosure and / or loss of such Personal Information.

10.2 Removing and Downloading Personal Information on to portable devices from workplace equipment or taking soft copies of Personal Information off-site must be authorised in writing by the manager of the relevant department from where the information emanates and a copy of such authorisation sent to the Information Officer, and which removal will be subject to the following provisions:

10.2.1 the person removing the Personal Information must explain and justify the operational need for the removal in relation to the volume and sensitivity of the Personal Information and ensure that the details of the Persona Information being removed is documented and recorded under a "removal register";

10.2.3 the Personal Information to be removed must be strongly encrypted;

10.2.4 the person removing and using said data should only store the data necessary for their immediate needs and should remove the data as soon as possible once dealt with and such removal should be confirmed by way of a recordal in the removal register;

10.2.5 to avoid loss of encrypted data, or in case of failure of the encryption software, an unencrypted copy of the data must be held in a secure environment;

10.3 Where it is necessary to store Personal Information on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by the Company all Company employees and where applicable, Operators and persons acting on behalf of The Company without exception must before storing said Personal Information ensure that the data is encrypted and is kept secure and that appropriate measures and safeguards are in place to prevent unauthorised access, disclosure and loss of such Personal Information and points 10.2.1- 10.2.5 will apply to said data.

10.4 Where soft copies of Personal Information are removed from Company premises, all Company employees and where applicable, Operators and persons acting on behalf of The Company without exception must before removing said Personal Information ensure that only that data necessary for the purpose it is being removed is taken, is documented in a removal register and is thereafter whilst away from Company premises kept safe and secure

and that appropriate measures and safeguards are in place to prevent unauthorised access, disclosure and loss of such Personal Information .

10.5 Soft copies of Personal Information and portable electronic devices housing Personal Information should be stored in locked units, and they should not be left on desks overnight or in view of third parties.

10.6 Personal Information which is no longer required should be securely archived and retained, with consideration for the format and retention period requirements relating to the data and destroyed when no longer required, all to be done in line with the Company Records Management and Archive Policy and procedures.

10.7 Personal Information must not be disclosed unlawfully to any third party.

10.8 Transfers of Personal Information to third parties as per the provisions of clause 9, must be authorised in writing by the manager of the relevant department from where the information emanates and a copy of such authorisation sent to the Information Officer. Furthermore, such transfer must be protected by adequate contractual provisions or data processor agreements, as set out under clause 9 above.

10.9 All losses of Personal Information must be reported to the relevant manager of the department from where the information emanates, the departmental Data Protection Coordinator and the Information Officer.

10.10 Negligent loss or unauthorised disclosure of Personal Information, or failure to report such events, may be treated as a disciplinary matter.

10.11 The Company via its Information Officer and IT department, where applicable, will continuously review its security controls and processes to ensure that all Personal Information is secure.

11. ACCESS AND CORRECTION OF PERSONAL INFORMATION

11.1 Any person has the right to access their Personal Information which the Company holds about them, provided that they follow the right to access procedure set out under the Company's PAIA Manual which can be obtained here www.iemsa.co.za.

11.2 Any person will also have the right to ask the Company to update, correct or delete their Personal Information on reasonable grounds by completing the relevant form found under the Company's PAIA Manual which can be obtained here www.iemsa.co.za.

11.3 Any person has the right to object to the Company processing their Personal Information which the Company currently holds about them, by filing a notice of objection, which is found under The Company's PAIA Manual which can be obtained here www.iemsa.co.za, which objection must be brought to the attention of the Information Officer.

11.4 Once a Person objects to the processing of their Personal Information, the Company may no longer process said Personal Information.

11.4 The details of the Company Information Officer is set out at the back of this Policy.

12. RECORDS MANAGEMENT

12.1 Records in all formats containing Personal Information must be created, safely and securely stored and disposed of in accordance with the Company's Records management and archiving Policy and any associated procedures and codes of practice in place from time to time.

12.2 All records of Personal Information must be authentic, reliable and usable and capable of speedy and efficient retrieval.

12.3 All records of Personal Information must not be retained for periods longer than the periods permitted below unless there is a specific reason there for and such retention is required for operational reasons.

12.4. The retention period for Personal Information is as follows:

12.4.1. Voter information, including the voter's roll, shall be retained for a period of one month. This information shall be retained for the purposes of allowing objections and auditing. In the event that objections lodged and/or auditing of election results is necessary, the information shall be retained for the extended period which it is required. The information shall be retained for a further month after the extended period, thereafter it shall be destroyed.

12.4.2. Employee information, shall be retained for the duration of employment. Upon termination of employment the information shall be retained for a period of 5 years.

12.4.3. In the case of casual or temporary workers, the information shall be retained for the period in which the work remains on standby, thereafter the information shall be retained for a period of 5 years. A worker shall not be deemed to be on standby if they remain inactive for a period of 12 months.

12.4.4. All other Personal Information shall be retained for a period of 5 years.

12.5. Upon the expiry of the retention period, the Personal Information in the possession of the Company shall be destroyed. This applies as follows:

12.5.1. In the event that the Personal Information is in hard-copy physical format it shall be destroyed by way of shredding or similar method which will render the Personal Information incapable of being recovered by any party. A certificate or invoice shall be sufficient proof of such disposal. Where this is not possible, the Information Officer along with one other party, shall sign the relevant Confirmation of Disposal form.

12.5.2. In the event that the Personal Information is in soft-copy digital format the device containing the information shall be destroyed by way of digital shredding, or where possible, the device containing the data shall be formatted multiple times or destroyed. A certificate or invoice shall be sufficient proof of such disposal. Where this is not possible, the Information Officer along with one other party, shall sign the relevant Confirmation of Disposal form.

12.6. The certificate, invoice, or Confirmation of Disposal form shall be *prima facie* proof of disposal and destruction.

13. ROLES AND RESPONSIBILITIES

13.1 Information Officer

The Company Information Officer has primary responsibility for the Company's compliance with POPIA. This comprises:

13.1.1 ensuring that the Company has a POPIA compliance program in place and that all employees and Operators, service providers, contractors and agents acting for or on behalf of The Company are aware of this Policy and their obligations in relation to the POPIA compliance program;

13.1.2 maintaining the Company's notification with the Regulator;

13.1.3 handling data subject access requests and requests from third parties for Personal Information;

13.1.4 promoting and maintaining awareness of POPIA and regulations, including training;

13.1.5 investigating losses and unauthorised disclosures of personal Information.

13.2 Heads of Department / Division

13.2.1 The Company Heads of Department / Divisions are responsible for ensuring their employees and where applicable all operators, service providers, contractors and agents acting for or on behalf of the Company understand the role of the Information Protection conditions in their day-to-day work, through induction, training and performance monitoring, and for monitoring compliance within their own areas of responsibility.

13.2.2 In the event that there is no Head of the Department due to the size of the Company or temporary vacancy, this role shall be fulfilled by the Information Officer.

13.3 Data Protection Coordinators

The Company Heads of Department / Divisions must ensure that Data Protection Coordinators are designated for their departments or divisions, and provided with

appropriate training and support. In the event that there is no Data Protection Coordinator due to the size of the Company or temporary vacancy, this role shall be fulfilled by the Head of the Department failing which it shall be fulfilled by the Information Officer. Coordinators are required to:

13.3.1 advise employees and where applicable Operators, service providers, contractors and agents acting for or on behalf of the Company in their departments on the implementation of and compliance with POPIA and this Policy and any associated guidance / codes of practice;

13.3.2 ensure appropriate technical and organisational measures are taken within their departments to ensure against unauthorised or unlawful processing of Personal Information and against accidental loss or destruction of, or damage to, Personal Information;

13.3.3 support the Company's notification with the Regulator by maintaining the register of holdings of Personal Information, including databases and relevant filing systems, and the purposes of processing;

13.3.4 keep the Information Officer informed of changes in the collection, use, and security of Personal Information within their department;

13.3.5 report any loss of Personal Information to the Head of Department / Division and the Information Officer;

13.3.5 ensure the proper completion of all section 18 informed consent documents.

13.4 Employees

All the Company employees, staff and contractors, regardless of term of employment or contract, are responsible for:

13.4.1 processing Personal Information in accordance with POPIA, the POPIA conditions for processing, and any guidelines and instructions issued by the Company from time to time;

13.4.2 ensuring that they only process Personal Information, which is relevant and accurate and only for the purpose for which it is required

13.4.3 ensuring that all special Personal Information will only be processed in line with the provisions set out under POPIA and in accordance with instructions set out by the Information Officer from time to time;

13.4.4 ensuring that all Personal Information and all records housing such Personal Information are safety retained, stored and archived and/ or destroyed when no longer required in accordance with the Company Records management and archiving Policy and procedures

13.4.5 complying with all security and monitoring measures in order to safeguard and protect any Personal Information which he or she may be in possession of;

13.4.6 ensuring that any transfer of Personal Information to third parties is authorised, lawful and that appropriate and safe transport mechanisms are employed in respect of the Personal Information so transferred such as encryption;

13.4.6 ensuring that only authorised downloading of electronic Personal Information onto portable devices or the removal of manual Personal Information from Company premises occurs;

13.4.7 raising any concerns in respect of the processing of Personal Information with the Information Officer;

13.4.8 promptly passing on to the Information Officer all data subject access requests and requests from third parties for Personal Information;

13.4.9 reporting losses or unauthorised disclosures of Personal Information to the Information Officer;

13.4.10 ensure the Personal Information they provide about themselves is up to date.

13.4.11 not attempt to gain access to information that is not necessary to hold, know or process.

13.5 Operators and service providers

13.5.1 All operators, service providers, contractors and agents acting for or on behalf of the Company have a responsibility to act only on the Company's instructions and to ensure that their processing of Personal Information provided to them by the Company is carried out strictly in compliance with this Policy, any operator agreement, and in accordance with POPIA and the eight data protection conditions housed under POPIA.

13.5.2 Where any employee asks any operators, service providers, contractors and / or agents to process Personal Information on behalf of the Company, such Employee must ensure that a written operator agreement is concluded with the aforementioned data processor which adequately addresses these responsibilities.

15. GENERAL

15.1 Any transgression of this Policy, will be investigated and may lead to disciplinary action being taken against the offender.

16. VERSION AND AMENDMENTS

16.1 This Policy is effective as of 15 December 2022.

16.2 The Company reserves the right to amend, update and revoke this Policy upon its discretion and without prior notice.

ANNEXURE A

INFORMATION OFFICER DETAILS

NAME: Nkululeko Tselane (Attorney of the High Court of South Africa)

TELEPHONE NUMBER: 083 657 2109

POSTAL ADDRESS: 72 Cavendish Street, Wendywood, Gauteng

E-MAIL ADDRESS: nkulueko@iemsa.co.za

HEAD OFFICE DETAILS

POSTAL ADDRESS: 72 Cavendish Street, Wendywood, Gauteng

PHYSICAL ADDRESS: 35 Ballyclare Drive, Bally Oaks Office Park, Bryanston, South Africa Johannesburg

E-MAIL ADDRESS: info@iemsa.co.za

WEBSITE: www.iemsa.co.za

ANNEXURE B

SECTION 18 INFORMED CONSENT DOCUMENT

CONSENT TO PROCESS PERSONAL INFORMATION

a) The Institute of Election Management Services in Africa ("the Company" or "IEMSA") declares that the processing of personal information and data is in compliance with The Protection of Personal Information Act no 4 of 2013 ("POPI") and in accordance with the professional and confidentiality requirements necessary in the course of business operations. The Company will only collect, process and further process personal information and special personal information consistent with the purpose for which it is required, and will be apparent from the context in which the information is requested.

b) We process personal information and/or special personal information and data, necessary for the implementation of our services, and for purpose of fulfilling our mandate, thus we process them for justifiable administration and the transaction of the contractual relationship.

c) The nature of the personal information and/or special personal information which is collected, processed and further processed relates to personal data and information which includes but it not limited to voter information, company information, name and surname, address, contact details, tax information, banking details, identity number, medical records and criminal records. Processing of information and data includes, but is not limited to collection, receipt, recording, collation, storage, updating or modification, retrieval, adaption or alterations, consultation, use provision, dissemination by means of transmission, distribution or making available in any other form, erasure or deletion of data and, the Company undertakes to only process the information in a manner adequate, relevant and not excessive in the context of the purpose for which it is processed.

d) The Client acknowledges that the personal information and/or special personal information supplied to the Company, has been collected directly from them or has been obtained with their consent and that the Client has further consented to its processing and further processing by the Company. Where the Client is providing another person's personal information and/or special personal information, the Client acknowledges that they have obtained such person's consent to the processing of their personal information.

e) The Company shall take such steps as may be required to ensure that it complies with any law in respect of transfer, storage, security, retention and use of the personal information and/or special personal information.

f) The Client acknowledges that the Company has the right to provide third parties with the Client's personal and special personal information and the Client gives their express consent to the disclosure of their personal data to third parties, which third parties shall include, but not be limited to, all domestic, national, foreign and international courts, state institutions, other authorities, private institutions, tribunals, and service providers.

g) The Client shall endeavour to keep the personal information and/or special personal information and data supplied to the Company up to date, and should any of the Client's details have changed, the Client is obliged to notify the Company of such change as soon as possible to ensure that the records of the Company are as accurate as possible.

h) The Client expressly consents to the processing of personal information and/or special personal information by way of the trans-border flow of information. This will occur where personal information has to be sent to parties involved in the Client's matters and/or service providers outside of the Republic of South Africa for processing and/or storage, and/or is necessary for the performance in terms of the contractual relationship. The Client understands that by agreeing to same that the information sent to another country might not be subject to the same legislation as it might not have similar information protection legislation in place.

i) All personal information and/or special personal information and data is contained in our office files and further saved and entered on our internal server in our office. It is stored within the provided and necessary extent until the end of the business relationship and for the extent of any legal compliance allowed and/or directed by law.

j) The Company has taken the necessary steps to ensure its compliance with generally accepted information security practices however data transmission on the internet can be subject to security gaps. Notwithstanding the technical and organisational security measures taken by the Company, manipulation by third parties or loss of data cannot be completely ruled out. In case of any data breach, we will promptly report to the affected person and the relevant authority.

SIGNED AT _____ ON _____ DAY OF _____ 20_____

_____
Company Name

_____
Name and Surname

_____
Signature