

Personal Information Act Policy for Erasmus Motaung Inc. – Version 3

**Company policy in terms of the Protection of Personal Information Act, as may
be amended at the time for Erasmus Motaung Inc.**

1. **Preamble**

- 1.1. The purpose of this policy is to assist the Private Body and the relevant Data Subject with a manner in which effect is given to a Data Subject's right to privacy subject to justifiable limitations which are aimed at protecting the Data Subject and / or the Private Body's rights and / or important interests.

2. **In this document**

- 2.1. **"Act [the]"**: The Protection of Personal Information Act, Act 4 of 2013.
- 2.2. **"Data Subject"**: means the person to whom Personal Information relates;
- 2.3. **"Information Officer"**: of a Private Body means the head of a Private Body as contemplated in section 1 of the Promotion of Access to Information Act;
- 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 the information contained in annexure **"A"** hereto.
- 2.5. **"Private Body"**: Erasmus Motaung Inc, Registration number: 1997/016580/21.
- 2.6. **"Processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including the activities referred to in Annexure **"B"**;
- 2.7. **"Record"** means any recorded information—

- 2.7.1. regardless of form or medium, including any of the following—
 - 2.7.1.1. Writing on any material;
 - 2.7.1.2. 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;
 - 2.7.1.3. 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;
 - 2.7.1.4. book, map, plan, graph or drawing;
 - 2.7.1.5. 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; and
 - 2.7.1.6. as per annexure “C” hereto.
- 2.7.2. in the possession or under the control of a Responsible Party;
- 2.7.3. whether or not it was created by a Responsible Party; and
- 2.7.4. regardless of when it came into existence;

2.8. **“Re-Identify”**, in relation to Personal Information of a Data Subject, means to resurrect any information that has been de-identified, that—

- 2.8.1. identifies the Data Subject;
- 2.8.2. can be used or manipulated by a reasonably foreseeable method to identify the Data Subject; or

2.8.3. can be linked by a reasonably foreseeable method to other information that identifies the Data Subject, and “**re-identified**” has a corresponding meaning;

2.9. “**Responsible Party**” means a Private Body or any other person which, alone or in conjunction with others, determines the purpose of and means for Processing Personal Information. The Private Body assigned its duties of a Responsible Party to the natural person identified as Emil Bihl, an employee of the Private Body.

3. **Section 19 Risk Assessment**

3.1. In order to secure the integrity and confidentiality of Personal Information in the possession and control of the Private Body, the Private Body undertake to take the appropriate, reasonable technical and organisational measures to prevent the loss of, damage to or unauthorised destruction of Personal Information and to prevent unlawful access to or processing of Personal Information.

3.2. To understand the Private Body’s obligation to achieve integrity and confidentiality of Personal Information in its possession and control, the Private Body conducted a risk assessment, which is attached hereto as annexure ‘**D**’.

4. **Controls**

4.1. The Private Body has control over Personal Information as follows:

- 4.1.1. Electronically via computers, software, internet and the cloud;
and
- 4.1.2. Hard copies of the records as recorded in annexure 'C' hereto.
- 4.2. The Private Body has a layered approach of control over Personal Information as follows:
 - 4.2.1. Attached as annexure 'E' is an organogram of the Private Body, which confirms that the Private Body effectually have three levels of layered controls, which are:
 - 4.2.1.1. Level 1: Employees conducting the day-to-day processing of Personal Information;
 - 4.2.1.2. Level 2: The Head of every department that has to verify and check that the employees performed their tasks and duties; and
 - 4.2.1.3. Level 3: Privileged access restricted to the Managing Director and Practice Manager.

4.3. People Controls

- 4.3.1. The Private Body controls its level 1 employees' access to the Personal Information as follows:
 - 4.3.1.1. Its code of conduct;
 - 4.3.1.2. Access is restricted to desk top computers only, which is password restricted to the specific employee; and
 - 4.3.1.3. May not take Records out of the office;

4.3.2. The Private Body controls its level 2 employees, being the various Heads of the departments' access to the Personal Information as follows:

4.3.2.1. The Heads of the department may take records home, and access Personal Information through their laptops and cell phones only. The Heads receive training on scam emails and the risks in using these devices.

4.3.3. The Private Body has to rely on its level 3 management, to act with the necessary honesty and integrity when using its privileged access.

4.4. Process controls

4.4.1. Annexure 'B' hereto records the processes. The level one employees are responsible for these processes.

4.4.2. The level 2 employees (Heads of Department) have sight on the progress of the matters, as the matters reach their milestones and are then responsible for checking that processing of the Personal Information have been done in line with the Private Body's policy and relevant legislation.

4.4.3. Level 3 employees will only be required to use their specialised access, in the event, that they suspect a Head of a department failing to act as required, or when a level 1 employee or a client raises any concerns over the processing of its information.

5. **Audit function**

5.1. Level 3 employees have access to audit functions on the processing of Personal Information with the assistance of the Private Body's ITC Consultant.

6. **Incident management Procedures**

6.1. All employees, departments will receive training on identifying a situation where Personal Information have been compromised and the procedure to follow, by notifying the Data Subject of the breach, consequences and potential risks, as well as the reporting thereof to the Regulator.

7. **Training**

7.1. Annual training will be provided on the Act, the Promotion to Access of Information Act and all aspects relating thereto.

8. **Rights of Data Subjects**

8.1. A Data Subject has the following rights:

- 8.1.1. To be notified that Personal Information about him, her or it is being collected; or
- 8.1.2. To be notified that his, her or its Personal Information has been accessed or acquired by an unauthorised person;
- 8.1.3. To establish whether a Responsible Party holds Personal Information of that Data Subject and to request access to his, her or its Personal Information;
- 8.1.4. To request, where necessary, the correction, destruction or deletion of his, her or its Personal Information;

- 8.1.5. To object, on reasonable grounds relating to his, her or its particular situation to the Processing of his, her or its Personal Information;
- 8.1.6. To object to the Processing of his, her or its Personal Information:
 - 8.1.6.1. at any time for purposes of direct marketing;
 - 8.1.6.2. not to have his, her or its Personal Information Processed for purposes of direct marketing by means of unsolicited electronic communications;
- 8.1.7. not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated Processing of his, her or its Personal Information intended to provide a profile of such person;
- 8.1.8. to submit a complaint to the Regulator regarding the alleged interference with the protection of the Personal Information of any Data Subject or to submit a complaint to the Regulator in respect of a determination by an adjudicator;
- 8.1.9. to institute civil proceedings regarding the alleged interference with the protection of his, her or its Personal Information

9. **Exclusions**

- 9.1. The Processing of Personal Information does not include the following:
 - 9.1.1. in the course of a purely personal or household activity;
 - 9.1.2. that has been de-identified to the extent that it cannot be re-identified again;

- 9.1.3. the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such Personal Information;
- 9.1.4. relating to the judicial functions of a court referred to in section 166 of the Constitution.

10. **Lawfulness of Processing**

10.1. Personal Information must be Processed:

- 10.1.1. lawfully; and
- 10.1.2. in a reasonable manner that does not infringe the privacy of the Data Subject.

11. **Minimality**

11.1. Personal Information may only be Processed if, given the purpose for which it is Processed, it is adequate, relevant and not excessive.

12. **Consent, justification and objection**

12.1. Personal Information may only be Processed if:

- 12.1.1. the Data Subject or a competent person where the Data Subject is a child consents to the Processing;
- 12.1.2. Processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party;

- 12.1.3. Processing complies with an obligation imposed by law on the Responsible Party;
 - 12.1.4. Processing protects a legitimate interest of the Data Subject;
 - 12.1.5. Processing is necessary for the proper performance of a public law duty by a public body;
 - 12.1.6. Processing is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom the information is supplied; or
 - 12.1.7. Executing the instructions of a Client.
- 12.2. The Responsible Party bears the burden of proof for the Data Subject's or competent person's consent.
- 12.3. The Data Subject or competent person may withdraw his, her or its consent, at any time: Provided that the lawfulness of the Processing of Personal Information before such withdrawal will not be affected.
- 12.4. A Data Subject may object, at any time, to the Processing of Personal Information:
- 12.4.1. on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such Processing; or
 - 12.4.2. for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.
- 12.5. If a Data Subject has objected to the Processing of Personal Information in terms the Responsible Party may no longer Process the Personal Information.

13. **Collection directly from Data Subject**

13.1. Personal Information must be collected directly from the Data Subject.

13.2. It is not necessary to comply with paragraph 13.1 if:

- 13.2.1. the information is contained in or derived from a public record or has deliberately been made public by the Data Subject;
- 13.2.2. the Data Subject or a competent person where the Data Subject is a child has consented to the collection of the information from another source;
- 13.2.3. collection of the information from another source would not prejudice a legitimate interest of the Data Subject;
- 13.2.4. collection of the information from another source is necessary:
 - 13.2.4.1. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
 - 13.2.4.2. 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);
 - 13.2.4.3. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
 - 13.2.4.4. in the interests of national security; or

- 13.2.4.5. to maintain the legitimate interests of the Responsible Party or of a third party to whom the information is supplied;
- 13.2.5. compliance would prejudice a lawful purpose of the collection;
or
- 13.2.6. compliance is not reasonably practicable in the circumstances of the particular case.

14. **Collection for specific purpose**

- 14.1. Personal Information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Responsible Party.
- 14.2. Steps must be taken to ensure that the Data Subject is aware of the purpose of the collection of the information. Therefore, it is included in all the mandates of the various departments.

15. **Retention and restriction of records**

- 15.1. Subject to subsections (2) and (3), 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:
 - 15.1.1. retention of the record is required or authorised by law;
 - 15.1.2. the Responsible Party reasonably requires the record for lawful purposes related to its functions or activities;
 - 15.1.3. retention of the record is required by a contract between the parties thereto; or

- 15.1.4. the Data Subject or a competent person where the Data Subject is a child has consented to the retention of the record.
- 15.2. Records of Personal Information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes if the Responsible Party has established appropriate safeguards against the records being used for any other purposes.
- 15.3. A Responsible Party that has used a record of Personal Information of a Data Subject to make a decision about the Data Subject, must:
 - 15.3.1. retain the record for such period as may be required or prescribed by law or a code of conduct; or
 - 15.3.2. 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.
- 15.4. 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 in terms of subsection (1) or (2).
- 15.5. The destruction or deletion of a record of Personal Information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.
- 15.6. The Responsible Party must restrict Processing of Personal Information if:

- 15.6.1. its accuracy is contested by the Data Subject, for a period enabling the Responsible Party to verify the accuracy of the information;
 - 15.6.2. 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;
 - 15.6.3. the Processing is unlawful and the Data Subject opposes its destruction or deletion and requests the restriction of its use instead; or
 - 15.6.4. the Data Subject requests to transmit the personal data into another automated Processing system.
- 15.7. Personal Information referred to in subsection (6) may, with the exception of storage, only be Processed for purposes of proof, or with the Data Subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such Processing is in the public interest.
- 15.8. Where Processing of Personal Information is restricted pursuant to subsection (6), the Responsible Party must inform the Data Subject before lifting the restriction on Processing.

16. **Further Processing to be compatible with purpose of collection:**

- 16.1. Further Processing of Personal Information must be in accordance or compatible with the purpose for which it was collected in terms of section 13.

- 16.2. To assess whether further Processing is compatible with the purpose of collection, the Responsible Party must take account of:
- 16.2.1. the relationship between the purpose of the intended further Processing and the purpose for which the information has been collected;
 - 16.2.2. the nature of the information concerned;
 - 16.2.3. the consequences of the intended further Processing for the Data Subject;
 - 16.2.4. the manner in which the information has been collected; and
 - 16.2.5. any contractual rights and obligations between the parties.
- 16.3. The further Processing of Personal Information is not incompatible with the purpose of collection if:
- 16.3.1. the Data Subject or a competent person where the Data Subject is a child has consented to the further Processing of the information;
 - 16.3.2. the information is available in or derived from a public record or has deliberately been made public by the Data Subject;
 - 16.3.3. further Processing is necessary:
 - 16.3.3.1. to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
 - 16.3.3.2. 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);
- 16.3.3.3. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
- 16.3.3.4. in the interests of national security;
- 16.3.4. the further Processing of the information is necessary to prevent or mitigate a serious and imminent threat to:
- 16.3.4.1. public health or public safety; or
- 16.3.4.2. the life or health of the Data Subject or another individual;
- 16.3.5. 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
- 16.3.6. the further Processing of the information is in accordance with an exemption granted under section 37.

17. **Quality of information**

- 17.1. A Responsible Party must take reasonably practicable steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary.
- 17.2. In taking the steps referred to in subsection (1), the Responsible Party must have regard to the purpose for which Personal Information is collected or further Processed.

18. **Documentation**

18.1. 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.

19. **Notification to Data Subject when collecting Personal Information**

19.1. If Personal Information is collected, the Responsible Party must take reasonably practicable steps to ensure that the Data Subject is aware of:

19.1.1. the information being collected and where the information is not collected from the Data Subject, the source from which it is collected;

19.1.2. the name and address of the Responsible Party;

19.1.3. the purpose for which the information is being collected;

19.1.4. whether or not the supply of the information by that Data Subject is voluntary or mandatory;

19.1.5. the consequences of failure to provide the information;

19.1.6. any particular law authorising or requiring the collection of the information;

19.1.7. the fact that, where applicable, the Responsible Party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

19.1.8. any further information such as the:

19.1.8.1. recipient or category of recipients of the information;

- 19.1.8.2. nature or category of the information;
- 19.1.8.3. existence of the right of access to and the right to rectify the information collected;
- 19.1.8.4. the existence of the right to object to the Processing of Personal Information as referred to in section 11 (3); and
- 19.1.8.5. right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be Processed, to enable Processing in respect of the Data Subject to be reasonable.

19.2. The steps referred to in subsection (1) must be taken:

- 19.2.1. 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
- 19.2.2. in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

19.3. A Responsible Party that has previously taken the steps referred to in subsection (1) complies with subsection (1) 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.

19.4. It is not necessary for a Responsible Party to comply with subsection (1) if:

- 19.4.1. the Data Subject or a competent person where the Data Subject is a child has provided consent for the non-compliance;
- 19.4.2. non-compliance would not prejudice the legitimate interests of the Data Subject as set out in terms of this Act;
- 19.4.3. non-compliance is necessary:
 - 19.4.3.1. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
 - 19.4.3.2. 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);
 - 19.4.3.3. for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or
 - 19.4.3.4. in the interests of national security;
- 19.4.4. compliance would prejudice a lawful purpose of the collection;
- 19.4.5. compliance is not reasonably practicable in the circumstances of the particular case; or
- 19.4.6. the information will:
 - 19.4.6.1. not be used in a form in which the Data Subject may be identified; or
 - 19.4.6.2. be used for historical, statistical or research purposes.

20. **Security measures on integrity and confidentiality of Personal Information**

20.1. 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:

20.1.1. loss of, damage to or unauthorised destruction of Personal Information; and

20.1.2. unlawful access to or Processing of Personal Information.

20.2. In order to give effect to subsection (1), the Responsible Party must take reasonable measures to:

20.2.1. identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

20.2.2. establish and maintain appropriate safeguards against the risks identified;

20.2.3. regularly verify that the safeguards are effectively implemented; and

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

20.3. 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.

20.4. Attached to this Policy is the Section 19 Risk Assessment in terms of the Protection of Personal Information Act in which the assessment was done.

21. **Information Processed by operator or person acting under authority**

21.1. An operator or anyone Processing Personal Information on behalf of a Responsible Party or an operator, must:

21.1.1. Process such information only with the knowledge or authorisation of the Responsible Party; and

21.1.2. treat Personal Information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

22. **Security measures regarding information Processed by operator**

22.1. A Responsible Party must, in terms of a written contract between the Responsible Party and the operator, ensure that the operator which Processes Personal Information for the Responsible Party establishes and maintains the security measures referred to in section 19.

22.2. The operator must notify the Responsible Party immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person.

23. **Notification of security compromises**

23.1. 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:

- 23.1.1. the Regulator;
 - 23.1.2. subject to subsection (3), the Data Subject, unless the identity of such Data Subject cannot be established; and
 - 23.1.3. any external stakeholders relevant to the Data Subject.
- 23.2. The notification referred to in subsection (1) 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.
- 23.3. 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.
- 23.4. The notification to a Data Subject referred to in subsection (1) must be in writing and communicated to the Data Subject in at least one of the following ways:
- 23.4.1. Mailed to the Data Subject's last known physical or postal address;
 - 23.4.2. sent by e-mail to the Data Subject's last known e-mail address;
 - 23.4.3. placed in a prominent position on the website of the Responsible Party;
 - 23.4.4. published in the news media; or
 - 23.4.5. as may be directed by the Regulator.

23.5. The notification referred to in subsection (1) must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including:

23.5.1. a description of the possible consequences of the security compromise;

23.5.2. a description of the measures that the Responsible Party intends to take or has taken to address the security compromise;

23.5.3. a recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise; and

23.5.4. if known to the Responsible Party, the identity of the unauthorised person who may have accessed or acquired the Personal Information.

23.6. 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.

24. **Access to Personal Information**

24.1. A Data Subject, having provided adequate proof of identity, has the right to:

- 24.1.1. request a Responsible Party to confirm, free of charge, whether or not the Responsible Party holds Personal Information about the Data Subject; and
- 24.1.2. 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:
 - 24.1.2.1. within a reasonable time;
 - 24.1.2.2. at a prescribed fee, if any;
 - 24.1.2.3. in a reasonable manner and format; and
 - 24.1.2.4. in a form that is generally understandable.
- 24.2. If, in response to a request in terms of subsection (1), 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.
- 24.3. If a Data Subject is required by a Responsible Party to pay a fee for services provided to the Data Subject in terms of subsection (1) (b) to enable the Responsible Party to respond to a request, the Responsible Party:
 - 24.3.1. must give the applicant a written estimate of the fee before providing the services; and
 - 24.3.2. may require the applicant to pay a deposit for all or part of the fee.
- 24.4.

- 24.4.1. A Responsible Party may or must refuse, as the case may be, to disclose any information requested in terms of subsection (1) 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.
- 24.4.2. 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.
- 24.5. 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 (4) (a), every other part must be disclosed.

25. **Correction of Personal Information**

- 25.1. A Data Subject may, in the prescribed manner, request a Responsible Party to:
- 25.1.1. 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
- 25.1.2. 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.
- 25.2. On receipt of a request in terms of subsection (1) a Responsible Party must, as soon as reasonably practicable:
- 25.2.1. correct the information;

- 25.2.2. destroy or delete the information;
 - 25.2.3. provide the Data Subject, to his or her satisfaction, with credible evidence in support of the information; or
 - 25.2.4. 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.
- 25.3. If the Responsible Party has taken steps under subsection (2) 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.
- 25.4. The Responsible Party must notify a Data Subject, who has made a request in terms of subsection (1), of the action taken as a result of the request.

26. **Manner of access**

- 26.1. 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.

27. **Prohibition on Processing of special Personal Information**

27.1. A Responsible Party may, subject to section 27, not Process Personal Information concerning:

27.1.1. 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

27.1.2. the criminal behaviour of a Data Subject to the extent that such information relates to:

27.1.2.1. the alleged commission by a Data Subject of any offence; or

27.1.2.2. any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

28. **General authorisation concerning special Personal Information**

28.1. The prohibition on Processing Personal Information, as referred to in section 26, does not apply if the:

28.1.1. Processing is carried out with the consent of a Data Subject referred to in section 26;

28.1.2. Processing is necessary for the establishment, exercise or defence of a right or obligation in law;

28.1.3. Processing is necessary to comply with an obligation of international public law;

28.1.4. Processing is for historical, statistical or research purposes to the extent that:

28.1.4.1. the purpose serves a public interest and the Processing is necessary for the purpose concerned;
or

28.1.4.2. it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the Processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;

28.1.5. information has deliberately been made public by the Data Subject; or

28.1.6. provisions of sections 28 to 33 are, as the case may be, complied with.

28.2. The Regulator may, subject to subsection (3), upon application by a Responsible Party and by notice in the *Gazette*, authorise a Responsible Party to Process special Personal Information if such Processing is in the public interest and appropriate safeguards have been put in place to protect the Personal Information of the Data Subject.

28.3. The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2).

29. **Authorisation concerning Data Subject's race or ethnic origin**

29.1. The prohibition on Processing Personal Information concerning a Data Subject's race or ethnic origin, as referred to in section 26, does not apply if the Processing is carried out to:

- 29.1.1. identify Data Subjects and only when this is essential for that purpose; and
- 29.1.2. comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

30. **Authorisation concerning Data Subject's health or sex life**

30.1. The prohibition on Processing Personal Information concerning a Data Subject's health or sex life, as referred to in section 26, does not apply to the Processing by:

- 30.1.1. medical professionals, healthcare institutions or facilities or social services, if such Processing is necessary for the proper treatment and care of the Data Subject, or for the administration of the institution or professional practice concerned;
- 30.1.2. insurance companies, medical aid schemes, medical scheme administrators and managed healthcare organisations, if such Processing is necessary for:
 - 30.1.2.1. assessing the risk to be insured by the insurance company or covered by the medical scheme and the Data Subject has not objected to the Processing;
 - 30.1.2.2. the performance of an insurance or medical scheme agreement; or
 - 30.1.2.3. the enforcement of any contractual rights and obligations;

- 30.1.3. schools, if such Processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
- 30.1.4. any public or private body managing the care of a child if such Processing is necessary for the performance of their lawful duties;
- 30.1.5. any public body, if such Processing is necessary in connection with the implementation of prison sentences or detention measures; or
- 30.1.6. administrative bodies, pension funds, employers or institutions working for them, if such Processing is necessary for:
 - 30.1.6.1. the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the Data Subject; or
 - 30.1.6.2. the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.
- 30.2. In the cases referred to under subsection (1), the information may only be Processed by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the Responsible Party and the Data Subject.
- 30.3. A Responsible Party that is permitted to Process information concerning a Data Subject's health or sex life in terms of this section and is not subject

to an obligation of confidentiality by virtue of office, profession or legal provision, must treat the information as confidential, unless the Responsible Party is required by law or in connection with their duties to communicate the information to other parties who are authorised to Process such information in accordance with subsection (1).

30.4. The prohibition on Processing any of the categories of Personal Information referred to in section 26, does not apply if it is necessary to supplement the Processing of Personal Information concerning a Data Subject's health, as referred to under subsection (1) (a), with a view to the proper treatment or care of the Data Subject.

30.5. Personal Information concerning inherited characteristics may not be Processed in respect of a Data Subject from whom the information concerned has been obtained, unless:

30.5.1. a serious medical interest prevails; or

30.5.2. the Processing is necessary for historical, statistical or research activity.

30.6. More detailed rules may be prescribed concerning the application of subsection (1) (b) and (f).

31. **Prohibition on Processing Personal Information of children**

31.1. A Responsible Party may, subject to section 35, not Process Personal Information concerning a child.

32. **General authorisation concerning Personal Information of children**

32.1. The prohibition on Processing Personal Information of children, as referred to in section 34, does not apply if the Processing is:

32.1.1. carried out with the prior consent of a competent person;

32.1.2. necessary for the establishment, exercise or defence of a right or obligation in law;

32.1.3. necessary to comply with an obligation of international public law;

32.1.4. for historical, statistical or research purposes to the extent that:

32.1.4.1. the purpose serves a public interest and the Processing is necessary for the purpose concerned;
or

32.1.4.2. 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

32.1.5. of Personal Information which has deliberately been made public by the child with the consent of a competent person.

32.2. 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.

32.3. 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:

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

32.3.1.1. review the Personal Information Processed; and

32.3.1.2. refuse to permit its further Processing;

32.3.2. provide notice:

32.3.2.1. regarding the nature of the Personal Information of children that is Processed;

32.3.2.2. how such information is Processed; and

32.3.2.3. regarding any further Processing practices;

32.3.3. 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

32.3.4. establish and maintain reasonable procedures to protect the integrity and confidentiality of the Personal Information collected from children.

33. **Duties and responsibilities of Information Officer**

33.1. An information officer's responsibilities include:

- 33.1.1. the encouragement of compliance, by the body, with the conditions for the lawful Processing of Personal Information;
 - 33.1.2. dealing with requests made to the body pursuant to this Act;
 - 33.1.3. working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;
 - 33.1.4. otherwise ensuring compliance by the body with the provisions of this Act; and
 - 33.1.5. as may be prescribed.
- 33.2. Officers must take up their duties in terms of this Act only after the Responsible Party has registered them with the Regulator.

34. **Designation and delegation of deputy information officers**

- 34.1. 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:
- 34.1.1. 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
 - 34.1.2. 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.

35. **Processing subject to prior authorisation**

- 35.1. The Responsible Party must obtain prior authorisation from the Regulator, in terms of section 58, prior to any Processing if that Responsible Party plans to:
- 35.1.1. Process any unique identifiers of Data Subjects:
 - 35.1.1.1. for a purpose other than the one for which the identifier was specifically intended at collection; and
 - 35.1.1.2. with the aim of linking the information together with information Processed by other responsible parties;
 - 35.1.2. Process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
 - 35.1.3. Process information for the purposes of credit reporting; or
 - 35.1.4. Transfer special Personal Information, as referred to in section 26, or the Personal Information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the Processing of Personal Information as referred to in section 72.
- 35.2. The provisions of subsection (1) may be applied by the Regulator to other types of information Processing by law or regulation if such Processing carries a particular risk for the legitimate interests of the Data Subject.
- 35.3. This section and section 58 are not applicable if a code of conduct has been issued and has come into force in terms of Chapter 7 in a specific sector or sectors of society.
- 35.4. A Responsible Party must obtain prior authorisation as referred to in subsection (1) only once and not each time that Personal Information is received or Processed, except where the Processing departs from that

which has been authorised in accordance with the provisions of subsection (1).

36. **Responsible Party to notify Regulator if Processing is subject to prior authorisation**

- 36.1. Information Processing as contemplated in section 57 (1) must be notified as such by the Responsible Party to the Regulator.
- 36.2. Responsible parties may not carry out information Processing that has been notified to the Regulator in terms of subsection (1) until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.
- 36.3. In the case of the notification of information Processing to which section 57 (1) is applicable, the Regulator must inform the Responsible Party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.
- 36.4. In the event that the Regulator decides to conduct a more detailed investigation, it must indicate the period within which it plans to conduct this investigation, which period must not exceed 13 weeks.
- 36.5. On conclusion of the more detailed investigation referred to in subsection (4) the Regulator must issue a statement concerning the lawfulness of the information Processing.
- 36.6. A statement by the Regulator in terms of subsection (5), to the extent that the information Processing is not lawful, is deemed to be an enforcement notice served in terms of section 95 of this Act.

36.7. A Responsible Party that has suspended its Processing as required by subsection (2), and which has not received the Regulator's decision within the time limits specified in subsections (3) and (4), may presume a decision in its favour and continue with its Processing.

37. **Failure to notify Processing subject to prior authorisation**

37.1. If section 58 (1) or (2) is contravened, the Responsible Party is guilty of an offence and liable to a penalty as set out in section 107.

38. **Direct marketing by means of unsolicited electronic communications**

38.1. 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:

38.1.1. has given his, her or its consent to the Processing; or

38.1.2. is, subject to subsection (3), a customer of the Responsible Party.

38.2.

38.2.1. A Responsible Party may approach a Data Subject:

38.2.1.1. whose consent is required in terms of subsection (1) (a); and

38.2.1.2. who has not previously withheld such consent, only once in order to request the consent of that Data Subject.

- 38.2.2. The Data Subject's consent must be requested in the prescribed manner and form.
- 38.3. A Responsible Party may only Process the Personal Information of a Data Subject who is a customer of the Responsible Party in terms of subsection (1) (b):
- 38.3.1. if the Responsible Party has obtained the contact details of the Data Subject in the context of the sale of a product or service;
 - 38.3.2. for the purpose of direct marketing of the Responsible Party's own similar products or services; and
 - 38.3.3. 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:
 - 38.3.3.1. at the time when the information was collected; and
 - 38.3.3.2. 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.
- 38.4. Any communication for the purpose of direct marketing must contain:
- 38.4.1. details of the identity of the sender or the person on whose behalf the communication has been sent; and
 - 38.4.2. an address or other contact details to which the recipient may send a request that such communications cease.
- 38.5. **"Automatic calling machine"**, for purposes of subsection (1), means a machine that is able to do automated calls without human intervention.

39. **Automated decision making**

39.1. Subject to subsection (2), 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 credit worthiness, reliability, location, health, personal preferences or conduct.

39.2. The provisions of subsection (1) do not apply if the decision:

39.2.1. has been taken in connection with the conclusion or execution of a contract, and:

39.2.1.1. the request of the Data Subject in terms of the contract has been met; or

39.2.1.2. appropriate measures have been taken to protect the Data Subject's legitimate interests; or

39.2.2. is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of Data Subjects.

39.3. The appropriate measures, referred to in subsection (2) (a) (ii), must:

39.3.1. provide an opportunity for a Data Subject to make representations about a decision referred to in subsection (1); and

39.3.2. 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).

40. **Transfers of Personal Information outside Republic**

40.1. 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:

40.1.1. 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:

40.1.1.1. 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

40.1.1.2. 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;

40.1.2. the Data Subject consents to the transfer;

40.1.3. 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;

- 40.1.4. 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
- 40.1.5. the transfer is for the benefit of the Data Subject, and:
 - 40.1.5.1. it is not reasonably practicable to obtain the consent of the Data Subject to that transfer; and
 - 40.1.5.2. if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it.
- 40.2. For the purpose of this section:
 - 40.2.1. **“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
 - 40.2.2. **“group of undertakings”** means a controlling undertaking and its controlled undertakings.

Annexure “A”

Personal Information within the sphere of the Company:

1. Initial connection:

- 1.1. Telephone call: Personal identifiable Personal Information;
- 1.2. Walk-ins: Personal identifiable Personal Information and any other ancillary documents relating to the matter of the client;
- 1.3. E-mail: Personal identifiable Personal Information and any other ancillary documents relating to the matter of the client;
- 1.4. Electronic meeting: Personal identifiable Personal Information and any other ancillary documents relating to the matter of the client;
- 1.5. Auto allocation system of an instruction via Lexis Convey: Banker details, any other attorney details, client's name, surname, identity number, address, e-mail address, telephone number and financials.

- 2. A wide variety of other Personal Information in order to execute the instructions but not to the extent that it constitutes special Personal Information as per the Act.

Annexure “B”

Refers to the processing activities specifically linked to the Company:

1. Data capturing of documentation received via initial connection;
2. Creation of file;
3. Issuing of mandate documents;
4. Issuing of FICA documentation;
5. Issuing of bank confirmation notices;
6. Confirmation of mandate;
7. Processing of payments;
8. Measuring FICA information against FICA policy;
9. Personal Information is used to request further Personal Information relating to the matter and / or mandate received in order to allow EMI to execute its instructions;
10. All activities of EMI to execute the mandate and / or instructions of the Client;
11. Submission of Personal Information to third parties for the purpose of executing instructions and / or mandate of the Client;
12. Termination of mandate;
13. All documents relating to storage of information;
14. Once the statutory period of retaining the records have passed, all information is destroyed which relates to the deidentification of the Client;

Annexure “C”

Documents generated containing Personal Information:

1. Initial connection documentation (which may vary pending on the nature of the instruction);
2. Client file (hard copy);
3. Mandate documents;
4. FICA documents;
5. Bank confirmation notices;
6. Invoices and / or statements and / or quotes;
7. Any other ancillary documents provided by the client to allow EMI to execute its mandate;
8. All documents relating to the execution of instructions and / or mandate of the Client including such documents to third parties to execute instructions;
9. Termination of mandate documents;
10. All documents relating to storage of Personal Information;
11. All documents relating to the deidentifying of the Client.

ERASMUS MOTAUNG INC ORGANOGRAM



