B&M Analysts
POWERING COMPETITIVENESS

POLICY

Privacy and Protection of Personal Information

for

THE BMA GROUP

CONTENT

Clause **Page No**

1. Introduction

1.1 The BMA Group is a group of companies that provides innovative commercial and technical solutions for leading industrial sectors with the view to improve competitiveness, implement sustainable empowerment and enhance economic growth and job creation. In the course of its operations, it enters into transactions which may include the processing, use, disclosure and collection of Personal Information about its employees, clients, customers, partners and members of the public. It is obligated to comply with POPI.

1.2 The BMA Group is committed to processing data, and specifically Personal Information in an open, transparent, responsive and responsible manner.

2. Purpose and Scope

2.1 This Policy applies to the BMA Group, all of its subsidiaries, affiliates, business partners, trade divisions and employees, including Operators.

2.2 The purpose of this Policy is to demonstrate the BMA Group's commitment to safeguarding the Personal Information of all persons, including juristic persons where applicable, with whom it interacts and to ensure that the BMA Group and its employees comply with the requirements imposed by POPI.

2.3 In particular, the purpose is to establish an institution wide policy that will provide direction with respect to the manner of compliance, give effect to the right of privacy and at the same time, balance the right to privacy against other rights such as the right of access to information, the right to protect important interests such as the free flow of information, regulate the manner in which Personal Information may be processed and establish measures to ensure respect for, and to promote, enforce and fulfil the rights protected.

2.4 The Policy sets out the objectives and directives on applicable protocols within the BMA Group to maintain and uphold the legal requirements and conditions as set out in Chapter 3 of POPI, including the safeguards pertaining to information transactions and specifically when processing Personal Information. The BMA Group has aligned and developed its data protection strategies with its statutory obligation to effectively implement the reasonable and necessary technical, structural and organisational

measures and operational controls in accordance with the relevant national data legislation and internationally recognised information and communication technology (ICT) standards and recommendations.

2.5 The BMA Group is resolute in processing data in an open, lawful and transparent way. This Policy sets out the processes and procedures to align the BMA Group's business strategy and the applicable national legislation, i.e. POPI, in terms of processing Personal Information when it is collected, stored, used, disclosed and destroyed.

2.6 The BMA Group will only Process data for the clear, precise and specific purpose for which it is collected from the Data Subject.

2.7 The Policy has application to all stakeholders. It applies to all employees, service providers and administrators and any person handling Personal Information of customers, suppliers and employees of the BMA Group.

2.8 The Policy has application to all information transactions where data is processed, including but not limited to data being exchanged and/or transmitted and which may constitute and/or include Personal Information.

2.9 Parties to an information transaction must therefore understand and comply with this Policy. In the event that a party to such a transaction does not understand any part of this Policy, or has any questions regarding data compliance protocols, that party must approach the Information Officer of the relevant BMA Entity.

2.10 Data and Personal Information shall only be collected from Data Subjects who have business or other dealings with the BMA Group for *inter alia* administrative needs, conducting of business operations, and for legislative data compliance and risk analysis.

3. **Definitions**

In this Policy:

3.1 "**BMA Group**" means Benchmarking and Manufacturing Analysts SA (Pty) Ltd, registration no. 2004/028453/07, and all of its affiliates, business partners, Operators, subsidiaries and trading divisions, including each BMA Entity;

3.2 "**BMA Entity**" means each of those entities recorded in **Annexure F**;

3.3 "**Consent**" means any voluntary, specific and informed expression agreeing to the processing of Personal Information;

3.4 "**Data Subject**" means the person to whom the Personal Information relates and in relation to the BMA Group, Data Subject would include employees, customers, service providers and administrators and any other individual with whom the BMA Group may interact, from time to time, whether or not such person is a natural person or a juristic person;

3.5 "**De-identify**", in relation to Personal Information of a Data Subject, means to delete information that:

(a) identifies the Data Subject;

(b) can be used or manipulated by reasonably foreseeable method to identify the Data subject; or

(c) can be linked by a reasonable foreseeable method or other information that identifies a Data Subject,

and "**De-identified**" has a corresponding meaning;

3.6 "**Information Officer**" in accordance with section 1 of PAIA means, in respect of any BMA Entity:

(a) the chief executive officer or equivalent officer of that BMA Entity or any person duly authorised by that officer; or

(b) the person who is acting as such or any person duly authorised by such acting person;

3.7 "**Information Regulator**" means the information regulator established in terms of section 39 of POPI;

3.8 "**Operator**" means a person who processes Personal Information for or on behalf of the BMA Group in terms of a contract or mandate, without coming under the direct authority of the BMA Group;

3.9 "**PAIA**" means the Promotion of Access to Information Act;

3.10 "**Personal Information**" means information that could be used to identify a Data Subject and includes:

(a) race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language;

(b) education, medical history, financial history, criminal history, employment history;

(c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to a person (such as postal address);

(d) biometric information, including physical, psychological or behavioural characterisation including blood typing, finger printing, DNA analysis, retinal scanning and voice recognition;

(e) opinions, views, preferences of the Data Subject and opinions or views of another person about the Data Subject;

(f) correspondence; and

(g) a name;

3.11 "**Policy**" means this Data Privacy Policy;

3.12 "**POPI**" means the Protection of Personal Information Act, 4 of 2013;

3.13 "**Processing**", as it relates to processing of Personal Information, means any operation or activity, whether or not by automatic means, including:

(a) collecting, receipt, recording, organising, collating, storage, updating, modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution, or making available in any form;

(c) merging, linking, degrading, erasure or destruction;

and "**Process**" shall have a corresponding meaning;

3.14 "**Record**" means any recorded Personal Information, regardless of its form or medium, including any writing, electronic information, label, marking, image, film, map, graph, drawing, tape and that is in the possession, or under control, of a Responsible Party, irrespective of whether it has been created by the Responsible Party or not and regardless of when it came into existence;

3.15 "**Responsible Party**" means the applicable entity within the BMA Group, or an Operator, who engages in the act of Processing Personal Information;

3.16 "**Special Personal Information**" means personal information concerning:

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or

(b) the criminal behaviour of a Data Subject to the extent that such information relates to:

(i) the alleged commission by a Data Subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings; and

3.17 "**Unique Identifier**" means any identifier that is assigned to a Data Subject and is used by the BMA Group for the purposes of its operations and which uniquely identifies the Data Subject in relation to the BMA Group.

4. <u>Lawful Processing of Information</u>

4.1 The BMA Group collects and receives information from a number of sources, including the following:

(a) directly from the Data Subject;

(b) during the course of the BMA Group's interactions with the Data Subject;

(c) when the Data Subject visits the premises of members of the BMA Group;

(d) when the Data Subject visits and/or interacts with the BMA Group's website or any other social media platforms or IT services;

(e) from publicly available sources; and

(f) from a third party who is authorised to share that information.

4.2 Personal Information may also be generated in the course and scope of the BMA Group's operational activities and in the fulfilment of obligations and duties as specified in contracts with its customers, service providers, business partners and if applicable, any other party, including Operators, to an information transaction where Personal Information is being transferred. The BMA Group's processing protocols are aligned with the conditions set out in Chapter 3 of POPI.

4.3 The BMA Group may Process the Personal Information for, *inter alia*, the following purposes:

(a) to verify the Data Subject's identity;

(b) to assess, enter into and/or perform a contract with the Data Subject, or the Data Subject's employer;

(c) for training and assessment purposes;

(d) for audit and record-keeping purposes;

(e) to confirm the Data Subject's credit worthiness and suitability as a customer or supplier;

(f) to comply with legal, regulatory and/or contractual obligations;

(g) to enable the Data Subject to enter the BMA Group's premises;

(h) to undertake security and monitoring the measures;

(i) to provide advertising, marketing and the media services to the Data Subject;

(j) to defend any legal claims in connection with the Data Subject contract with the relevant the member of the BMA Group or for the BMA Group to establish, bring or pursue a claim against the Data Subject; or

(k) otherwise for the BMA Group's legitimate interests or those of a third party.

4.4 Where it is lawful and practicable for the BMA Group to allow it, the Data Subject has the right not to identify himself when dealing with the BMA Group. However, if the Data Subject does not provide the BMA Group with his/her Personal Information, it may impact the BMA Group's ability to engage with the Data Subject and/or provide services to the Data Subject.

4.5 Chapter 3 of POPI stipulates 8 (eight) provisions for the lawful Processing of information namely accountability, processing limitation, purpose specification, further processing, information quality, openness, security safeguards and Data Subject participation.

4.6 Any employee, service provider or administrator must ensure that:

(a) all Personal Information of employees, service providers and stakeholders is Processed in accordance with the 8 (eight) standards for the lawful Processing of information; and

(b) no Special Personal Information or Personal Information concerning a child is Processed unless the express prior consent of a competent person is first obtained. In the event that either of these categories of information is required to be Processed and it is not possible to first obtain prior written consent, the matter shall be referred to the Information Officer for direction.

4.7 Failure to adhere to these provisions may result in disciplinary or other action being taken.

4.8 In the course of information transactions, certain information may be collected by the BMA Group which may be held and labelled as Special Personal Information. Special Personal Information will only be collected where necessary for the purpose for which it

is being collected and with the Data Subject's Consent, unless such collection is demanded and/or authorised by law.

5. **Rights of Data Subjects**

5.1 The BMA Group respects a Data Subject's right to have his or her or its Personal Information Processed lawfully.

5.2 Data Subjects have the right:

(a) to be notified that Personal Information about him, her or it is being collected or that his, her or its Personal Information has been accessed or acquired by an authorised person;

(b) to establish whether the BMA Group holds Personal Information of that Data Subject and to request access thereto;

(c) to request, where necessary, the correction, destruction or deletion of his, her or its Personal Information;

(d) to object, on reasonable grounds relating to his, her or its particular situation to the Processing of his, her or its Personal Information;

(e) to object to the Processing of his, her or its Personal Information at any time for the purposes of direct marketing;

(f) not to be subject, under certain circumstances, to a decision which is based solely on the basis of automated Processing of his, her or its Personal Information intended to provide a profile of such a person;

(g) to submit a complaint to the Regulator regarding the alleged interference with the protection of his, her or its Personal Information; and

(h) to institute civil proceedings regarding the alleged interference with the protection of his, her or its Personal Information.

5.3 To the extent that the legal basis for the BMA Group to process a Data Subject's Personal Information is informed consent, the Data Subject has the right to withdraw

such consent at any time. If the Data Subject's consent is required for further transactions, then such a request must be clear, concise and specific to the use of the service or product for which it is provided.

5.4 Consent, whenever it is obtained, should cover all Processing activities carried out for a specific purpose or purposes. When the Processing has multiple purposes, Consent should be given for each such purpose.

5.5 Withdrawal of Consent will not affect the lawfulness of Processing which occurred prior to such withdrawal.

5.6 All Data Subjects participating in information transactions with the BMA Group are entitled to exercise any of their rights by clear, concise communication by email to the Information Officer.

5.7 Data Subjects furthermore have the right to object to Processing of their Personal Information for scientific or historical research purposes or statistical purposes on grounds relating to such Data Subject's situation or circumstances, unless the Processing is necessary for the performance of a task which is carried out for reasons of public interest.

6. **Accountability**

6.1 The BMA Group holds ultimate responsibility to ensure that the provisions of POPI are complied with for the collection, retention, dissemination and use of the Personal Information.

6.2 This places substantial and ultimate accountability on the BMA Group, employees, service providers and administrators to ensure that Personal Information is processed in a lawful manner.

6.3 The BMA Group remains responsible for the Processing of information regardless of whether or not the information is passed on to a third party (such as an administrator) or not; provided that agreements must be concluded with those third parties in terms of which they agree to be bound by and comply with the requirements of this Policy and of POPI. Notwithstanding this, the BMA Group's website may contain links to other websites. The BMA Group will not be held liable for the privacy controls of third-party

websites. Data Subjects may be associated with a unique identifier, which may leave traces which, when combined with other information received by the third-party websites, could be used to create profiles of the Data Subjects and identify them.

6.4 In order to ensure that the provisions of POPI are adhered to by employees, service providers and Operators, each BMA Entity will appoint an Information Officer, and register that Information Officer with the Regulator.

6.5 A substantial amount of Personal Information is in electronic form. Employees, service providers and administrators of the BMA Group are responsible for information technology and providing the tools to manage and safeguard information.

6.6 Employees, managers, supervisors, service providers and administrators are accountable to the BMA Group to report any breaches in data security and to ensure that any risks of breaches are identified and reported.

7. **Processing Limitation**

7.1 The Personal Information must be processed lawfully and in a reasonable manner, which does not infringe the privacy of the Data Subject.

7.2 The notion of reasonableness incorporates the requirements of balance and proportionality. Employees, service providers and administrators must therefore take into account the interests and reasonable expectations of Data Subjects as well as all of the provisions which are incorporated in these conditions.

7.3 The Processing must be adequate, relevant and not excessive given the purpose for which it is processed.

7.4 Subject to the provisions of section 11(1) of POPI, the Data Subject must consent to the processing of the Personal Information. Where necessary, the consent must be voluntary and clear, however, it does not have to be in writing. Employees, service providers and administrators must ensure that the Data Subject has provided consent when they request Personal Information.

7.5 The Data Subject may at any time withdraw consent, on reasonable grounds, to the processing of its Personal Information. If a Data Subject withdraws consent, the

Personal Information must be deleted or De-identified so that it will no longer be associated with that Data Subject.

7.6 The Processing must be necessary to carry out the actions for the conclusion or performance of a contract to which the Data Subject is a party.

7.7 The Processing must protect a legitimate interest of the Data Subject, and the Processing must be necessary for pursuing the legitimate interest of the BMA Group.

7.8 The Personal Information must be collected directly from the Data Subject, except if:

(a) the Personal Information is a matter of public record;

(b) the Data Subject has consented to the collection of the Personal Information from another source;

(c) the collection of the Personal Information from another source would not prejudice a legitimate interest of the Data Subject;

(d) the collection of the Personal Information is necessary by law;

(e) compliance would prejudice a lawful purpose of the collection; or

(f) compliance is not reasonably practicable in the circumstances.

8. **Purpose Specification**

8.1 The collection of the Personal Information must be for a specific expressly defined purpose, examples of which purposes are recorded in clause 4.3, above.

8.2 The purpose of the collection and Processing of Personal Information influences every aspect of the processing of the information, the manner of its collection, periods of retention, further processing, disclosure to third parties and any further issues which may apply.

8.3 While the BMA Group will have a duty to notify the Regulator of its purposes and functions, the factor determining the purpose for the collection of Personal Information will always be the specified purpose communicated to the Data Subject.

8.4 The Data Subject must be made aware of the purpose. This enables the Data Subject to make an informed decision as to whether the Personal Information should be made available to the Responsible Party. The purpose for the collection of the Personal Information should be explained to the Data Subject, either telephonically or by inclusion in the relevant documentation exchanged between the parties, including, for example, the customer application form and/or trading terms and conditions. Examples of the purposes for which Personal Information is obtain are recorded in clause 4.3, above.

8.5 Records of Personal Information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or Processed. The BMA Group will determine, with regard to the circumstances surrounding the collection of the Personal Information, the length of time personal records are to be kept for and implement procedures in order to ensure that records are destroyed or De-identified when no longer required.

8.6 The Data Subject must consent in the event that the Personal Information is kept for a period which is longer than necessary for achieving the purpose for which the information was collected. This can be done by way of a contractual arrangement such as provision to this effect in the customer application form and/or trading terms and conditions.

8.7 Where Personal Information is disclosed to Operators as referred to in clauses 13.3 and 13.4 below, such disclosure will only be insofar as is reasonably necessary for the maintenance and completion of business and operational functions.

8.8 The BMA Group will ensure that its Customer Contracts are in compliance with the contents of this Policy and the relevant data legislation.

9. **Further Processing**

9.1 Any further processing of the Personal Information must be compatible with the purpose for which the Personal Information was initially collected.

9.2 For example, if the BMA Group collects Personal Information for the purposes of providing services to a customer, the information cannot be Processed further for the purpose of profiling and marketing products to that customer. The only exception to this is if the Data Subject consents to such use.

9.3 To assist in determining whether further Processing is compatible with the initial purpose of collection, the employee, service provider or administrator must take account of:

(a) the relationship between the purpose for which the Personal Information was originally collected and the intended purpose of any further Processing;

(b) the nature of the Personal Information concerned;

(c) the consequences of further processing;

(d) the manner in which the Personal Information was collected; and

(e) contractual rights and obligations between the parties.

9.4 Personal Information may be Processed by the BMA Group where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for such Processing is the Responsible Party's legitimate interest in the protection and assertion of the Responsible Party's rights, a Data Subject's rights and the legitimate interest(s) of any other person(s).

9.5 Personal Information may be Processed by the BMA Group where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for such Processing is the legitimate interest of the BMA Group in diligently protecting its business from risk.

9.6 Financial transactions relating to the BMA Group websites and services may be handled by its payment service providers such as recognised financial institutions. The BMA Group will share transaction data with such service providers only to the extent necessary for the purposes of processing payments, refunding of payments, and dealing with complaints and queries relating to payments and refunds.

10. **Information Quality**

10.1 The employee, service provider or administrator responsible for the Processing of the Personal Information must take reasonable steps to ensure that the Personal Information remains complete, is accurate, is not misleading and is updated where necessary.

10.2 In essence this condition requires that appropriate Personal Information security measures safeguarding the integrity of the Personal Information be employed.

11. **Openness**

11.1 The Personal Information must be Processed in a transparent and fair manner.

11.2 The Data Subject must be provided with information which allows the Data Subject to be aware that Personal Information is being collected, the identity of the Responsible Party, the purpose for the collection of the information and whether the supply of the information by the Data Subject is voluntary or mandatory.

11.3 Further, the party responsible for the Processing of the information, whether it be the employee, service provider, Operator or administrator, must maintain all documentation of the Processing operations.

12. **Security Safeguards**

12.1 The BMA Group, as well as all Responsible Parties undertake to ensure that the appropriate controls are in place to ensure that confidential, internal and Personal Information is disclosed only to those who are authorised and who have a legitimate business related need for such access.

12.2 The BMA Group will take all reasonable steps to establish and maintain sufficient security controls, technological and organisational, to ensure that the all Personal Information which is Processed by the BMA Group is protected against unauthorised alteration, destruction and/or access that may change the integrity of the Personal Information and that it is backed up and stored in a format which is readily accessible by the BMA Group.

(a) The backup solution utilised by the BMA Group is designed and based on the principles of lawful Processing and retention policies as set out in the relevant data legislation.

(b) The IT Backup Policy sets out the processes and procedures for authorised access to information. These policies are in compliance with the relevant data legislation and adherence thereto will be strictly enforced.

(c) The BMA Group furthermore has made provision for procedures and responses in the event of data breach incidents in its IT Disaster Policy.

12.3 The party responsible for the Processing of the Personal Information, if not the BMA Group (but an Operator), must ensure that the integrity of the Personal Information remains secure against loss, destruction or unlawful access.

12.4 Any service provider, administrator or third-party Processing Personal Information for the BMA Group, must do so only with the knowledge and express authorisation of the BMA Group and must treat the Personal Information as strictly confidential.

12.5 Employees, managers, supervisors, service providers and administrators have a duty to ensure that Personal Information is not mislaid or inadvertently disclosed by, for example, leaving it displayed on a computer screen or leaving printouts at the printer.

12.6 Any Personal Information which is Processed or accessed outside the office premises of the BMA Group must be encrypted to guard against theft.

12.7 Where Personal Information is to be moved to another country in order for business activities to be conducted, the interested and/or authorised parties must consult with their departmental manager, the Data Subject(s) concerned, as well as the Information Officer in order to ensure compliance with POPI and any further applicable legislation, with particular reference to Consent and jurisdictional complications.

12.8 Should the BMA Group receive unsolicited Personal Information, it will assess whether it is Personal Information which it is entitled or authorised to collect and Process. If the Personal Information is that which the BMA Group is authorised to collect and Process, it will treat this Personal Information in accordance with the principles set out in this Policy. If the Personal Information is not capable of being collected and Processed by the BMA Group, it shall destroy or De-Identify the Personal Information as soon as is practicable.

12.9 The BMA Group’s automated information technology back-up solution is designed and implemented in accordance with accepted and effective security standards controls and daily monitoring alerts. In the event of data which is no longer to be retained and when lawfully able to do so, it will be destroyed and De-Identified as soon as practicably

possible and/or upon specific request by completion of the requisite Form 2 a copy of which is attached to this Policy as Annexure **D**.

12.10 All hard copies of documents must be shredded once the documents are no longer required.

12.11 Once the Personal Information is no longer required or no longer authorized, the records must be destroyed, deleted or De-identified. Records may be kept longer for historical, statistical or research purposes and the appropriate safeguards must be implemented against the use of the records for any other purposes, provided that the consent of the Data Subject is obtained.

13. Disclosure of Information

13.1 The Responsible Parties shall make all reasonable efforts to ensure that the parties to information transactions agree on non-disclosure provisions and consent to transactions which are within the scope of his/ her/ its specific mandate.

13.2 The BMA Group will not disclose Personal Information for purposes other than the purpose for which it was collected (the "**Primary Purpose**") unless:

(a) the Data Subject has consented thereto;

(b) the secondary use or disclosure is related to the Primary Purpose, in the case of Personal Information which is not Special Personal Information, or is directly related to the Primary Purpose, in the case of Personal Information which is Special Personal Information; or

(c) it is otherwise required or authorised by or under law or a court/tribunal order.

13.3 It may at times be necessary for the BMA Group to disclose Personal Information to third parties, including Operators and/or service providers and as may be permitted or required by law. Where this is the case, the BMA Group will enter into a written agreement with the Responsible Party and/or third party.

13.4 An agreement such as that referred to in clause 13.3 must contain an assurance from the Operator or service provider, as the case may be, that such Operator or service provider will at a minimum, subscribe, match and adhere to the same prescriptions and

restrictions pertaining to the processing of Personal Information as is required by the relevant data legislation and this Policy, and that it has adequate or equivalent infrastructure and organisational measures in place which are in accordance with accepted industry standards, and that it will Process Personal Information in strict accordance with an issued mandate and specified instructions from the BMA Group only.

13.5 The BMA Group reserves the right to disclose Personal Information to any member of the group of companies which comprises the BMA Group, together with all of its subsidiaries, partners and affiliates.

13.6 If the recipient of Personal Information is not the BMA Group (including its related entities, subsidiaries and trading divisions) then such recipient must be verified as a legitimately interested party and confirm whether the Personal Information is required for the legitimate performance of tasks within the competence of the recipient. The grounds for the request must be verified by the BMA Group, as well as the recipient's competence to receive the Personal Information.

13.7 The necessity of the transmission of Personal Information as referred to in clause 13.6 will be evaluated together with the recipient's organisational and technical security safeguards and measures as required by law and by this Policy.

13.8 The BMA Group may disclose Personal Information to its insurers and/or professional advisors insofar as is reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

13.9 Operators must enter into a data transfer agreement which is subject to limitations on the condition of further Processing and secondary Processing regarding the obtaining of Consent from the Data Subject.

13.10 All requests for confidential, internal or Personal Information which originate from a person or entity outside of the BMA Group must be forwarded to the Information Officer or any such duly authorised and appointed representative.

13.11 All requests for confidential, internal or Personal Information which fall outside of the standard business practice or procedure and which originate from an employee of the

BMA Group must be forwarded to the human resources department of the BMA Group for employee authentication and thereafter to the Information Officer and/or the employee's line manager as may be necessary for final authorisation.

13.12 Requests referred to in clause 13.11 must be reasonably considered by the Information Officer and/or the employee's line manager, as the case may be, and further directives must be issued on the approval thereof.

14. **Data Subject Participation**

14.1 The Data Subject has the right to request the BMA Group to confirm, free of charge, whether the BMA Group holds Personal Information about the Data Subject.

14.2 The Data Subject may request the BMA Group to provide it with a description of the Personal Information held by it or by a third party within a reasonable time. Any fees charged for providing the Data Subject with the information required shall not be excessive. The BMA Group should also advise the Data Subject that the Personal Information may be corrected upon request.

14.3 The Data Subject has a right to access the Personal Information and request a correction or deletion of the Personal Information. The BMA Group, employees, service providers and administrators each have a duty to report such a request to the Information Officer. Any such request must be forwarded to the Information Officer or his or her duly authorised representative.

14.4 Where the Data Subject is an employee, any requests to correct Personal Information must be directed at the Data Subject's line manager, the human resources department of the BMA Group and the Information Officer.

14.5 If there are circumstances where the BMA Group believes that the information is accurate and no agreement between the Data Subject and the BMA Group can be reached to amend the information, the BMA Group is obliged to link the Personal Information in dispute, in such a manner that it will always be read, with an indication that the correction of the Personal Information has been requested by the Data Subject but has not been made.

14.6 In instances where changes have been made which may impact on decisions taken using Personal Information, POPI imposes a duty on the BMA Group to advise, if reasonably practical, any third parties to whom the information may have been disclosed.

14.7 The BMA Group, as a Responsible Party, will only use Personal Information for direct marketing with the Data Subject's Consent. Such Consent will be obtained either:

(a) in writing, by requesting completion of a prescribed form (Annexure **E**) which must be returned to the BMA Group; or

(b) electronically, by requesting the Data Subject to tick an electronic box on email, or otherwise, it being recorded that the relevant provisions of Annexure **E** are to be complied with.

14.8 Data Subjects retain the right to object to the BMA Group's processing of Personal Information in terms of section 11(3) of POPI. If such an objection is made, the BMA Group will cease to process such Data Subject's Personal Information.

15. **Breach of Policy**

15.1 Failure to comply with the rules and standards set out in this Policy, and those policies which have been incorporated by reference herein, may be regarded as a transgression of company policy and must be reported to the relevant Information Officer.

15.2 Incidents of any breach of this Policy must be reported immediately to the relevant Information Officer by email. The Information Officer must investigate the breach accordingly and notify the relevant Information Regulator as may be appropriate, necessary and applicable.

15.3 Where there are reasonable grounds to believe that Personal Information has been accessed, acquired, destroyed or altered by any unauthorised person, the Responsible Party must notify the Information Regulator and the Data Subject(s), unless the identity of the Data Subject(s) cannot be established.

15.4 Where there are reasonable grounds to believe that Personal Information has been accessed, acquired, destroyed or altered by any unauthorised person, notifications will

be actioned and sent to the Data Subject(s) concerned, unless the identity of the Data Subject(s) cannot be established, in which case a notification will be published on the BMA Group website. Such notification must also be sent via email, as soon as is reasonably possible after discovery of the compromise and to enable a Data Subject to take pre-emptive measures as may be available and/or appropriate, taking into account the legitimate needs of law enforcement and any measures which may be necessary to determine the scope of the compromise and to restore the integrity of the Responsible Party's Records.

16. **Policy Maintenance**

The BMA Group shall review this Policy at least every (3) three years or more frequently as needed to respond to changes in the regulatory and legislative environment, as well as technological advancement in privacy protection.

Annexure A: Rights of Data Subjects

Section 5 of POPI states that a Data Subject has the right to have his, her or its Personal Information Processed in accordance with the conditions for the lawful Processing of Personal Information, including the right:

- to be notified that:
    - Personal Information about them is being collected as provided for in terms of section 18; or
    - their Personal Information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;
- to establish whether a Responsible Party holds Personal Information of that Data Subject and to request access to their Personal Information as provided for in terms of section 23;
- to request, where necessary, the correction, destruction or deletion of their personal information as provided for in terms of section 24;
- to object, on reasonable grounds relating to their particular situation to the processing of their personal information as provided for in terms of section 11(3)(a);
- to object to the processing of their personal information:
    - at any time for purposes of direct marketing in terms of section 11(3)(b); or
    - in terms of section 69(3)(c);
- not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1);
- not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of their personal information intended to provide a profile of such person as provided for in terms of section 71;
- 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 of an adjudicator as provided for in terms of section 74; and
- to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99.

Annexure B: POPIA Guide to the BMA Group Employees

The following principles for the protection of personal information of Data Subjects must be applied by all the BMA Group employees:

1. Email addresses of participants on group emails must be blind copied to prevent unauthorised distribution of email addresses;

2. Internal email trails must be removed from emails when communicating externally;

3. Employee and customer information may not be used for purposes other than those of the BMA Group;

4. Confidential information must be locked away;

5. Confidential information must not be left on unattended desks or on printers;

6. No personal information may be forwarded to a third party without the express written permission of the Data Subject;

7. Third party service providers responsible for the protection of information must sign and agree to this policy.

Annexure C: Information Officers Responsibilities

1. Attending on this Policy and POPI is to occur at regular intervals so that all employees are made aware of the Policy and POPI.

2. Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information or any other action so required in terms of POPI.

3. Every employee currently employed by the BMA Group will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or other action, as so required, in terms of POPI.

4. The BMA Group archived client information which is stored onsite which is also governed by POPI, and access to these areas is limited to authorised personnel.

5. Where the BMA Group supplies other third-party service providers with Personal Information, they will be required to sign a service level agreement guaranteeing their commitment to POPI.

6. All electronic files or data are backed up by the BMA Group IT division which is also responsible for system security that protects third party access and physical threats.

7. A manual is to be prepared in terms of PAIA, placed on the BMA Group's website and published in the Government Gazette.

Annexure D: Form 2

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	

B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY; and or** **REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.** *(Please provide detailed reasons for the request)*

Signed at ..... this ..... day of .....20……...

.....
Signature of data subject/ designated person

Annexure E: Form 4

FORM 4

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 6]

TO: _____

_____

_____

_____

(Name of data subject)

FROM: _____

_____

_____

_____

Contact number (s): _____

Fax number: _____

E-mail address: _____

(Name, address and contact details of responsible party)

Full names and designation of person signing on behalf of responsible party:

_____

.....

Signature of designated person

Date: _____

PART B

I, _____ *(full names of data subject)* hereby:

☐ Give my consent.

To receive direct marketing of goods or services to be marketed by means of electronic communication.

SPECIFY GOODS or SERVICES:

_____

_____

SPECIFY METHOD OF COMMUNICATION:

FAX:
E-MAIL:
SMS:
OTHERS – SPECIFY:

Signed at …… this ……. day of ……. 20 …..

……
Signature of data subject

Annexure F: BMA Entities

1. B and M Analysts (Pty) Ltd, registration no. 2013/045141/07;

2. Benchmarking and Manufacturing Analysts (Pty) Ltd, registration number 2004/028453/07;

3. BMA Intelligent Systems (Pty) Ltd, registration number 2011/116643/27;

It is recorded that, for the avoidance of doubt, the list of BMA Entities may be subject to change from time to time. An updated list of the BMA Entities may be obtained from BMA Head Office on contact number 031 764 6100 or requested by email to legal@bmanalysts.com;