

BMI SOUTH AFRICA DATA PRIVACY POLICY

Version 1.0, 16 June 2022, Group Legal

| | |
|--|--------|
| 1. Preamble | PAGE 3 |
| 2. Definitions | PAGE 3 |
| 2.1 PERSONAL DATA/ DATA SUBJECT | |
| 2.2 PROCESSING OF PERSONAL DATA | |
| 2.3 CONTROLLER/ PROCESSOR | |
| 2.4 PERSONAL DATA BREACH | |
| 3. Scope of this Policy | PAGE 4 |
| 4. Scope of the GDPR | PAGE 4 |
| 5. Principles of Data Processing | PAGE 4 |
| 6. Accountability | PAGE 5 |
| 7. Information Obligations | PAGE 5 |
| 8. Data Retention | PAGE 5 |
| 9. Data Security | PAGE 5 |
| 10. Rights of Data Subjects | PAGE 6 |
| 11. Personal Data Breaches/ Notification Obligations | PAGE 7 |

| | |
|--|--------|
| 12. Processing on behalf of the Controller | PAGE 7 |
| 13. Special Categories of Personal Data/ Data Relating to Criminal Convictions/ Data of Children | PAGE 7 |
| 14. Fines under the GDPR/ Civil Liability | PAGE 8 |
| 15. GDPR | PAGE 8 |
| 16. Contact | PAGE 8 |

1. Preamble

BMI Group¹ ("BMI") takes data protection and data privacy very seriously. Therefore, BMI wants to ensure that you, BMI's employees and contractors, are well informed about the data protection law requirements affecting our company. In particular, BMI wants to be sure that all personal information that BMI processes, or that is processed on BMI's behalf, is handled in a manner that is compliant with all applicable data protection laws. All BMI employees and contractors are responsible for processing personal data in BMI's possession according to this policy and applicable data protection law requirements.

Accordingly, please be advised that on 25 May 2018, the EU General Data Protection Regulation ("GDPR") will take effect. GDPR provides a uniform set of rules for the processing of personal data throughout the European Union ("EU"). This policy will give you a summary of the GDPR regulations. Please note, that in addition to the requirements of GDPR, there may be legislation in your local jurisdiction that must also be complied with. If you have questions regarding specific jurisdictions' data protection laws please contact privacy@standardindustries.com.

Summary of GDPR Regulations:

2. Definitions

This "Definitions" section provides those key GDPR definitions used and referred to in this policy. To the extent a term used in this policy is undefined, please refer to the GDPR, and in particular Article 4.

To the extent that legislation in your local jurisdiction applies, the definitions used and referred to in this policy, and any analogous terms shall have the means and definitions set out in the respective local legislation.

2.1 PERSONAL DATA/ DATA SUBJECT

Personal data means any information related to an identified or identifiable natural person, and in the event that the Protection of Personal Information Act 4 of 2013 ("POPIA") applies, an identifiable, existing juristic person ("data subject"). An identifiable natural person and/or juristic person (where applicable) is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, and identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person or juristic person (where applicable).

2.2 PROCESSING OF PERSONAL DATA

Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.3 CONTROLLER/PROCESSOR

A controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, that determines the purposes and means of the processing of personal data. A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

1

Please find more information about BMI Group and its operating companies here: www.bmigroup.com

2.4 PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Scope of this Policy

This privacy policy applies to all employees and contractors of BMI located in South Africa. All processing of personal data by BMI and on behalf of BMI, in South Africa, must be conducted in compliance with this privacy policy and applicable data protection laws. This privacy policy shall apply in South Africa only, and in the event of any conflict or inconsistency between these guidelines and the BMI group wide policies which regulate the same or similar processing activities, these guidelines will prevail to the extent of such conflict of inconsistency.

4. Scope of the GDPR

The GDPR applies first and foremost to EU establishments that act as personal data controllers and processors in connection with their business activities and operations. In certain cases, the GDPR's provisions also apply to data controllers or processors outside of the EU, and in particular those foreign-companies that control or process data in connection with:

- offering goods or services to data subjects in the EU, irrespective of whether payment by the data subject is required; or
- monitoring data subjects' behavior to the extent their behavior takes place within the EU.

5. Principles of Data Processing

The GDPR stipulates several principles related to processing personal data.

BMI is implementing measures to ensure that the processing of personal data at BMI's complies with the following GDPR principles:

- **Lawfulness, fairness and transparency:** All personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation:** Personal data can be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimization:** Only such data can be processed in accordance with this principle that is adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed.
- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date.
- **Storage limitation:** Controllers and processors are only allowed to store personal data in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- **Integrity and Confidentiality:** All processing of personal data must ensure appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using

appropriate technical or organizational measures.

- **Accountability:** The controller is responsible for and must be able to demonstrate compliance with the other principles of data processing. Please see more about the principle of accountability in Section 6 of this policy.

6. Accountability

The above mentioned principle of accountability is one of the key principles of data processing under the GDPR. Accordingly, BMI intends to implement measures that demonstrate all processing of personal data is performed in accordance with the GDPR. All employees and contractors that process personal data on BMI's behalf should comply with all measures employed by BMI to ensure compliance with the aforementioned principles.

7. Information Obligations

When processing personal data of data subjects, BMI will inform the data subjects about such processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Articles 12 to 15 of the GDPR set forth comprehensive rights to information for data subjects and the duties of controllers to provide said information. Employees and contractors are expected to support BMI efforts to comply with its comprehensive information duties by providing BMI with all necessary information to keep data current and accurate.

8. Data Retention

Per the GDPR, all personal data must be deleted as soon as it is no longer necessary to achieve the purposes for which it was collected, except if a statutory provision requires differently. BMI will be implementing data retention guidelines that instruct employees and contractors on how to ensure that they do not process any personal data that is no longer necessary to achieve the purposes for which they were collected.

9. Data Security

The GDPR stipulates that data controllers and processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and in particular (as appropriate):

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

All employees of BMI must comply with those organizational measures that the company implements to safeguard personal data.

In particular, all BMI employees and contractors are responsible for safeguarding personal data by using password protection. Passwords must be changed regularly. The use of obvious passwords must be avoided and no employee or contractor is allowed to share the username, password or other details regarding the password protection of personal data with others or store such information in an insecure way.

10. Rights of Data Subjects

According to the GDPR, data subjects have specific legal rights related to BMI's processing of their personal data. BMI takes the rights of its data subjects very seriously. Therefore, all employees and contractors should respect the rights of the data subjects and must deal with their concerns adequately.

The following list contains information on data subjects' rights arising from applicable data protection laws:

- **Right to rectification:** Data subjects have the right to obtain from BMI rectification of personal data concerning them. BMI must make reasonable efforts to keep personal data in its possession or control accurate, complete, current and relevant, based on the most recent information available to BMI.
- **Right to restriction:** Data subjects have the right to restrict BMI's processing of their personal data, if
 - they contest the accuracy of their personal data for the period BMI needs to verify its accuracy,
 - the processing is unlawful and they request the restriction of processing rather than erasure of their personal data,
 - BMI no longer needs their personal data but the data subjects require the same for the establishment, exercise or defense of legal claims, or if
 - they object to the data's processing while BMI verifies whether BMI's legitimate grounds override theirs.
- **Right to access:** Data subjects have the right to receive information regarding the personal data BMI holds about them, including information as to which categories of personal data BMI has in its possession or control, what the data is being used for, where BMI collected the data, if not from the data subjects directly, and to whom the data has been disclosed, if applicable. Data subjects have the right to obtain from BMI one copy, free of charge, of personal data BMI holds about them.
- **Right to portability:** At the data subject's request, BMI must transfer their personal data to another controller, where technically feasible, provided that the processing is based on the data subject's consent or necessary for the performance of a contract. Rather than receiving a copy of the personal data, the data subject has the right to request that BMI transfer the data to another controller, specified by the data subject, directly.
- **Right to erasure:** Data subjects have the right to demand BMI erase their data, where
 - the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
 - they have a right to object further processing of their personal data (see below) and execute this right;
 - the personal data has been unlawfully processed;

Unless the processing is necessary

- for compliance with a legal obligation which requires processing by BMI;
- for statutory data retention requirements;

- for the establishment, exercise or defense of legal claims.
- **Right to object:** Data subjects have the right to object – at any time – to the processing of their personal data due to their particular situation, provided that the processing is not based on the data subject's consent but on BMI's legitimate interests or those of a third party. In this event BMI shall no longer process the data subject's personal data, unless BMI can demonstrate compelling legitimate grounds and an overriding interest for the processing or for the establishment, exercise or defense of legal claims. If the data subject objects to the processing, the data subject must specify if it wishes the erasure of the personal data or the restriction of its processing by BMI.

11. Personal Data Breaches/ Notification Obligations

BMI will, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify any personal data breach to the relevant supervisory authority. As an exception, there is no obligation to notify a personal data breach to the supervisory authority if the breach is unlikely to result in a risk to the personal rights and freedoms of the data subjects affected by the personal data breach.

Furthermore, if a personal data breach is likely to result in a high risk to the personal rights and freedoms of the affected data subjects, BMI must generally communicate the personal data breach to the data subjects without undue delay. As an exception, BMI may refrain from communicating the personal data breach if BMI eliminates any risks to the data subjects by implementing appropriate technical and organizational protection measures or by taking subsequent measures.

In the event that POPIA applies, BMI will, without undue delay and, where feasible, not later than 72 hours after becoming aware of reasonable grounds to believe that a personal data breach may occur or has occurred, notify (i) the South African Information Regulator; and (ii) the affected data subjects, unless the identity of such data subjects cannot be established.

Therefore, it is crucial for BMI to be informed about any personal data breaches without undue delay. Employees and contractors can contact BMI by writing an email to Privacy@standardindustries.com.

12. Processing on behalf of the Controller

In accordance with its obligations under GDPR, BMI will only use data processors that provide sufficient guarantees that they will implement those technical and organizational measures required by the GDPR and ensure the protection of the data subjects' rights. Further, the processing must be governed by a contract that is binding on the processor with regard to BMI and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of BMI. Employees and contractors of BMI can find a comprehensive list of requirements that such contract must stipulate in Article 28 Paragraph 3 of the GDPR.

13. Special Categories of Personal Data/ Data Relating to Criminal Convictions/ Data of Children

The processing of certain categories of personal data is subject to further GDPR requirements. Any processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data

concerning a natural person's sex life or sexual orientation can only be conducted under the requirements of Article 9 Paragraph 2 of the GDPR. The processing of personal data related to criminal convictions and offences is subject to Article 10 of the GDPR. If an employee or contractor of BMI is processing any of the above-mentioned special categories of personal data,

BMI plans to implement measures to ensure that the processing is compliant to the requirements of GDPR Articles 9 and 10.

BMI will not collect or process personal data belonging to children under 16 years absent parental consent, pursuant to applicable local law. If an employee or contractor of BMI becomes aware that BMI is processing any personal data of a child without respective parental consent, the employee or contractor must inform BMI without undue delay.

14. Fines under the GDPR/ Civil Liability

The GDPR imposes administrative fines of up to 4 % of the global turnover or EUR 20 million, whichever is higher. Smaller infringements are fined with up to 2 % of the global turnover and EUR 10 million. Such administrative fines can be imposed against controllers and/or processors of personal data. In addition, controllers and processors of personal data face possible civil claims regarding material and non-material damages. Employees and contractors of BMI should be aware of the possible consequences of failing to comply with GDPR data processing requirements.

15. GDPR

Employees and contractors can find the GDPR online at: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=DE>.

16. Contact

Any BMI employee or contractor can direct questions regarding the subject matter of data protection, this data privacy policy or any request in the exercise of his or her legal rights to:

Privacy@standardindustries.com

All requests to exercise individual legal rights provided by the GDPR should be brought to the attention of BMI's data protection officer. Employees and contractors of BMI can also contact the data protection officer directly by writing an e-mail to Privacy@Standardindustries.com.