POLICY & GUIDELINES

BMI Group South African Retention and Destruction of Personal Data Policy Effective: June 16, 2022

1. Intent

BMI Group and its subsidiaries (together, “BMI Group” or the “Company”) operate in countries around the world, including in the European Union (“EU”). On 25 May 2018, the EU General Data Protection Regulation (“GDPR”) will take effect. One goal of GDPR is to standardize data protection laws across EU members states.

The intent of this Policy is to ensure the proper retention and deletion of Personal Data (as defined below) in South Africa.

2. Scope

All Company employees, temporary staff, contractors, and consultants (“Users”) wherever located, are expected to comply with this Policy.

3. Policy

The Company’s policy is to ensure that all Personal Data is handled in a secure and legally compliant fashion (see below for definition of (“Personal Data”). Set forth below are guidelines that all Users must follow when managing the retention and destruction of Company information containing Personal Data. Local BMI Group offices may have additional document retention policies that apply to documents which do not contain Personal Data and which must also be complied with. To the extent that local laws impose obligations more stringent than those contained herein, the Company is obligated to comply with such laws. Questions regarding any conflict between this Policy and a local policy should be directed to Privacy@StandardIndustries.com.

To the extent that local laws and/or legislation applies, the definitions used and referred to in this policy, and any analogous terms shall have the meanings and definitions set out in the respective local legislation.

This 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.

Any User who fails to follow the below guidelines may be subject to dismissal, other disciplinary

action and/or damage claims.

4. Guidelines

As relevant to this Policy, GDPR Article 5 requires that Personal Data be collected for a specific purpose, and kept in a form that permits the identification of an individual for no longer than necessary for the purposes for which the Personal Data was processed. Similarly, Article 17 provides (among other items) that the Company has the obligation to delete Personal Data when it is no longer necessary to the purpose for which it was initially collected or processed.

The Company's retention and destruction of data will comply with applicable GDPR requirements as well as any other applicable local laws and regulations.

4.1 PERSONAL DATA

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).

4.2 RETENTION OF PERSONAL DATA

The Company will only retain information containing Personal Data for as long as legally permitted. Attached as Appendix A to this Policy is a schedule outlining the default retention periods for Company information containing Data Subjects' Personal Data. Appendix A will be regularly maintained and updated, and will be available to Users on the Company intranet site or can be requested by emailing Privacy@standardindustries.com. In some instances Personal Data may be retained for longer than set out in the Appendix if local laws require; details of any variation to the default retention periods set out in the Appendix can be obtained from Users' local HR teams.

Please see the Company Privacy Policy and relevant Privacy Notices for more information on how the Company or third-parties acting on its behalf process and handle Personal Data. Questions regarding the retention or processing of Personal Data by the Company or third-parties can be directed to Privacy@StandardIndustries.com.

4.3 DESTRUCTION OF PERSONAL DATA

When the Company no longer has a legally relevant reason to retain particular Personal Data, all media containing the data shall be rendered unreadable or otherwise destroyed in a secure manner.

Hard copy documents must be disposed of in confidential waste bins or securely shredded. Any questions regarding the secure destruction of hard copy documents should be directed to the applicable User's local HR team. Electronic data must also be disposed of securely. Questions regarding the secure destruction of electronic information should be directed to a local member of the Information Security or Information Technology teams.

BMI Group requires that any third-parties handing User Personal Data provide adequate assurances of their compliance with applicable data protection laws, including GDPR. Questions related to third-party data protection agreements or third-party data retention or destruction can be directed to Privacy@StandardIndustries.com.

4.4 EXCEPTIONS

Exceptions to this Policy and standards set within must be legally permissible as well as documented and authorised by the BMI Group Compliance Committee. All exceptions shall be reviewed and resolved on a case by case basis.

5. Right to change the policy

This Policy does not form part of any employee's contract of employment or any other Users' terms of engagement with any company in the BMI Group and we reserve the right to modify, revoke, suspend, terminate or change this Policy in whole or in part, at any time, with or without notice, subject to applicable law.

APPENDIX A - Personal Data and HR Data Retention Guidelines

As a general rule, we delete Personal Data when it is no longer required for the purposes for which we process these Personal Data. The default retention periods below describe typical periods of time for which we store or otherwise process Personal Data. Depending on the circumstances, where Personal Data is needed for a shorter or longer period of time, it may be deleted earlier or later. Please note that the potential need to defend against legal claims and particular local law requirements may require and permit longer retention on a case-by-case basis.

Record Category	**Default Retention Period**
Recruitment records. These may include: ● Completed online application forms or CVs ● Assessment exercises or tests ● Notes from interviews and short-listing exercises ● Pre-employment verification of details provided by the successful candidate (where permitted by local laws). For example, checking qualifications and taking up references. *These may be transferred to a successful candidate's employment file* ● Criminal records checks (where permitted by local laws). These may be transferred to a successful candidate's employment file only if they are strictly relevant to the ongoing relationship	6 months after notifying candidates of the outcome of the recruitment process.
Immigration checks, including copies of passports, residence permits and identification documents (where permitted by local laws)	While employment continues and up to three years after employment ceases.
Terms and conditions of employment. These may include: ● Contracts of employment ● Amendment letters ● Details of participation in bonus plans ● Details of benefit plans	While employment continues and up to six years after employment ceases.
Payroll and wage records. These may include: ● Payroll and wage records ● Details on overtime worked ● Details of bonuses paid ● Expenses you have claimed ● Benefits in kind provided to you	Six years from the financial year-end in which payments were made.

Social security, national insurance contribution records (or equivalent)	Not less than three years after the end of the tax year to which they relate.
Pension participation and contribution records	12 years from the ending of any benefit payable under the policy.
Bank account details	While employment continues (assuming salary paid directly into bank account) and for as long after employment as required to make final payments.
Personnel records and employment history. These may include: ● Consents for the processing of special categories of personal data ● Annual leave records ● Annual performance reviews ● Disciplinary procedures ● Grievance procedures ● Documents relating to resignation or termination	While employment continues and up to six years after employment ceases.
Any reportable accident, death or injury in connection with work	Three years from the date the report was made.
Sickness records	While employment continues and for six years after employment ceases.
Details of maternity, paternity and adoption leave. These may include: ● Details of payments made (statutory and contractual (if applicable)) and calculations ● Certificates to confirm pregnancy or adoption or other medical evidence	Three years after the end of the tax year in which the statutory period of leave ends.
Third party business partners' contact details	During term of relationship and for six years from date of termination of contractual relationship.
Details of customers' orders	Six years from date contract fulfilled.
Backup Media	Backup storage media may be retained within legal limits to ensure compliance with statutory and other IT security and data security requirements, e.g. according to Art. 32 GDPR.