POLICY & GUIDELINES

BMI South Africa Data Breach Policy & Guidelines
Effective: May 4, 2018

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. The goal of GDPR is to standardize data protection laws across EU members states.

The intent of this Policy is to explain the procedures that the Company and its Users (as defined below) must follow when handling a personal data breach

2. Scope

All Company employees, temporary staff, contractors, and consultants (“User”) located in South Africa, are expected to comply with this Policy.

3. Policy

The Company’s policy is to comply with all relevant laws and regulations, including GDPR and local data privacy laws and regulations. Set forth below are guidelines that the Company and all Users must follow when responding to and managing a personal data breach as required by GDPR Articles 33 and 34.

4. Guidelines

All personal data breaches at BMI will be investigated, managed, communicated and resolved in a structured and controlled way in compliance with GDPR. All Users must follow the following guidelines in order to assist the Company in managing personal data breaches. These guidelines 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.

4.1 DEFINITIONS

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) specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach: A personal data breach within this context means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Examples include misplacing hard copy personnel files, a breach into BMI"s network where Personal Data is stored, the loss, theft or unauthorized access to a Company device or account, or accidentally sending an email or electronic file which includes personal data to an unintended external contact. If you are unsure whether a data breach has occurred, you should report the incident without delay so the Company can understand if a breach has occurred or not and whether we need to report the incident (see below).

4.2 RESPONSE PROCESS

Identifying personal data breaches and understanding BMI‟s response plan are vital parts of User GDPR awareness and training. In addition to the information provided in this Policy, BMI offers Security Awareness Training, as well as mandatory GDPR Training to help Users identify personal data security breaches.

The following response process should be followed when responding to an actual or suspected personal data breach.

Step 1 – Recognize and Escalate

Upon discovering or suspecting a personal data breach, the identifying User must immediately document the relevant incident and notify their manager, the Company‟s General Counsel (+44 20 2757 1908) and Chief Compliance Counsel (Compliance@StandardIndustries.com), and the Company‟s Data Protection Officer, Sebastian Kraska (BMIGroup@iitr.de) of the breach.

Step 2 – Notify the Relevant Supervisory Authorities and Data Subjects

Upon receiving notice of a personal data breach, the relevant manager and DPO will work with members of the Legal, HR, and Information Security and Information Technology (collectively, “IT”) teams to communicate with the appropriate data protection or supervisory authority(ies), in addition to communicating the data breach to any affected data subjects as required by GDPR.

Users should not communicate with any supervisory or regulatory authority(ies) without direction from a member of the Legal team.

a) Notifying the Data Supervisory Authority

GDPR Article 33 requires that the relevant supervisory authority is informed within 72 hours of BMI becoming aware of a personal data breach incident resulting in a risk to the rights and freedoms of Data Subjects.

A breach that risks the rights and freedom of Data Subjects is outlined in Recital 75 of GDPR, and includes, among other items, a breach that may implicate data that could lead to discrimination, identity theft or fraud, financial loss, economic or social disadvantage, loss of control over personal data, criminal history, genetic information, and religious or group affiliation.

A breach that does not constitute a risk to the rights and freedoms of those Data Subjects whose personal data is affected is not relevant under GDPR and will not be reported to the data supervisory authority (ies) or the affected User(s).

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

When communicating a suspected or actual personal data breach to a supervisory authority, BMI Group will include the following information in the notice:

- describe the nature of the personal data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of BMI Group‟s Data Protection Officer and Chief Compliance Counsel, for obtaining further information;
- describe the likely consequences of the personal data breach; and
- describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In those circumstances where BMI Group is unable to notify a supervisory authority of a breach within 72 hours, BMI Group‟s notice to the authority shall be accompanied by reasons for the delay.

b) **Notifying the Affected Data Subjects**

In the case of a personal data breach that must be reported to a supervisory authority, affected Data Subjects will be advised of the data breach as detailed by the form attached as Exhibit A to this document or such suitable method as BMI Group determines. As required by GDPR Article 34, this notice will be provided without undue delay.

Step 3 – Investigate, Contain and Eradicate the Breach

Upon receiving notice of a personal data breach regardless of risk level, BMI Group‟s IT and Legal teams will work expeditiously to (1) identify the scope of the breach, (2) obtain all information pertinent to the breach, including relevant devices, log files, access records, and emails, (3) document those events that resulted in the breach, (4) document any actual or potential loss or damage to the Company or affected Users, (5) identify and document the root cause of the breach and those individuals or entities responsible. To the extent necessary, Legal and IT shall engage external experts to assist with the investigation of a breach.

Upon identifying the scope of the breach, BMI Group will work to prevent the breach from spreading in either scope or severity. Typically this can be achieved by isolating the affected data systems from unaffected data systems.

Once a breach is contained, BMI Group‟s IT team will work to correct the incident by addressing the systems at issue. To the extent necessary, Legal and HR will work with IT to correct any access control or physical control issues discovered.

Step 4 – Recover.

Once the breach has been investigated and resolved, BMI Group IT will work to restore any affected systems/processes to fully operational status and close the incident.

Step 5 – Documentation.

All personal data breaches regardless of risk level shall be documented by BMI Group IT, including the facts surrounding the breach, its effects and the remedial action taken.

4.3 EXTERNAL DATA BREACH RESPONSE PROCESS

In the event BMI Group is notified by a third-party of a personal data breach under GDPR Articles 33 or 34 that may affect its Users or other Data Subjects, BMI Group will notify the Users and supervisory authorities as required by law, and work with the relevant third-parties and authorities, to audit and eradicate the breach as outlined in Section 2 of this Policy, and as provided by any pertinent Data Protection Agreement or Security Guidelines.

4.4 EXCEPTIONS

Exceptions to this policy and standards set within must be documented and authorized by the BMI Group Compliance Committee. All exceptions shall be reviewed and resolved on a case by case basis.

5. Right to change 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 - user notification template for personal data breaches

[INDIVIDUAL NAME]

[STREET ADDRESS]

[CITY]

[POSTAL CODE]

[DATE]

Dear [INDIVIDUAL NAME]:

We are writing to let you know that there has been a personal data breach within the BMI Group that has potentially included your personal data. We respect the privacy of your information, which is why, as a precautionary measure, we are letting you know about this incident.

Details of the data breach

[Between/On] [IDENTIFY TIME PERIOD OF BREACH], [SUMMARIZE BREACH INCIDENT].] The data accessed [may have included/included] personal information such as [IDENTIFY TYPES OF PII INCLUDED SUCH AS NAME, ADDRESS, DOB]. To our knowledge, the data accessed did not include any [IDENTIFY TYPES OF PII NOT INVOLVED]].

Should you wish to find out more information about this incident or the steps we are taking to address it, please contact the BMI Group Compliance Team at Compliance@StandardIndustries.com.

Likely Consequences of the data breach

[Description of the likely consequences of the personal data breach]

BMI Group takes any personal data breach seriously, and as a result we have taken the following steps to address and remediate the breach:

[Insert Notification, Investigation and Remediation steps taken].

Please do not hesitate to contact the BMI Group Compliance Team with any questions or concerns.

Kind Regards,

[Insert Relevant IT or Legal Signatory]