DATA PRIVACY POLICY

Version 2.0 | 01 January 2023 | Group Legal

1. Preamble

BMI Group[1] (**"BMI"**) takes data protection and data privacy very seriously. Therefore, BMI wants to ensure that you, BMI's employees and independent contractors, are well informed about the data protection law requirements affecting our companies. In particular, BMI wants to be sure that all personal data 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. In this context, this Data Privacy Policy ("**Policy**") defines what diligence BMI employees ("**Employees**") and independent contractors ("**Contractors**") must conduct when processing Personal Data on BMI's behalf and when processing personal data in BMI's possession.

The EU General Data Protection Regulation (**"EU GDPR"**) and the UK Data Protection Act ("**UK GDPR**") (together the **"GDPR"**) underpin this Policy. GDPR provides a uniform set of rules for the processing of personal data throughout the EU and the UK.

Please note, that in addition to the requirements of GDPR, there may be more restrictive legislation in your local jurisdiction that must also be complied with. If you have questions regarding specific jurisdictions' data protection laws please contact Privacy@BMIGroup.com.

2. Scope of this Policy

This Privacy Policy applies to all BMI Employees and Contractors, unless there is local Privacy Policy that takes precedence. All processing of Personal data by BMI and on BMI's behalf must be conducted in compliance with this Privacy Policy and applicable Data Protection Laws.

3. Definitions

This 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.

3.1 PERSONAL DATA

"Personal data" is any information related to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an email address, an 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. This also includes less obvious details e.g. your BMI employee number.

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

3.2 SPECIAL CATEGORY OF PERSONAL DATA

“Special Category of Personal Data” or “Sensitive Data” are 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, data concerning a natural person's sex life or sexual orientation, or data involving criminal convictions.

3.3 PROCESSING

“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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. It is a very broad concept and includes almost any action you could take involving Personal data.

3.4 CONTROLLER/PROCESSOR

A “Controller” is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (i.e. decides the "why" and the "how").

A “Processor” is a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the Controller (i.e. follows the Controller's instructions).

BMI can be either, depending on the scenario.

3.5 PERSONAL DATA BREACH

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

4. Principles of Data Processing

The GDPR contains a number of principles related to processing personal data. BMI or the Contractor has implemented measures to ensure that the processing of Personal data 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 individual.
- **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 Data

minimization 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 unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**: The Controller is responsible for and must be able to demonstrate compliance with the other principles of data processing.

5. Accountability

The principle of accountability is one of the key principles of the GDPR. Accordingly, BMI has implemented measures that demonstrate all processing of Personal data is performed in accordance with the GDPR such as: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles (see Section 8 hereinafter), as well as having adequate resources and controls in place to ensure and to document GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
- implementing privacy by design when processing personal data and completing data protection impact assessments ("**DPIAs**") where processing presents a high risk to rights and freedoms of data subjects (see section 16);
- integrating data protection into internal documents including this data protection policy, related policies, privacy guidelines or privacy notices;
- regularly training personnel on the GDPR, this data protection policy and related policies and data protection matters including, for example, individual rights, consent, legal basis, DPIA and personal data breaches. BMI maintains a record of training attendance by BMI personnel; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

All BMI 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.

6. Information Obligations

When processing Personal data, BMI will inform the relevant individuals about such processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language. 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.

As part of its information obligations, BMI must explain how BMI processes personal data and how it applies data protection principles via a privacy notice. A privacy notice must contain certain information as required by GDPR. An example of a privacy notice covering the processing of data collected on our BMI websites and through other activities is our "Website Privacy Notice". We also have specific privacy notices covering processing of Personal data about our employees, visitors to our offices, customers and users of certain web platforms.

If Personal data is intended to be used for any purposes other than those which have been described to the individual in a privacy notice, this must be reviewed and approved by the BMI Compliance Team (Compliance@BMIGroup.com).

7. Data Retention

Data retention refers to the storing and use of data for a defined time period. Personal data should only be retained for as long as necessary for the purpose it was collected. Data retention must be stated in privacy notices (i.e. how long we intend to keep the personal data for the relevant purposes).

If you have a specific question about how long a category of personal data is retained, please contact us at privacy@bmigroup.com.

8. Data Security, integrity and confidentiality

The GDPR stipulates that Controllers and Processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

An example of a technical measure is BMI setting the below password requirements; an organisational measure would be our privacy governance structure. Such measures should include (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 organisational measures for ensuring the security of the processing.

All Employees and Contractors of BMI must comply with the measures that the company

implements to safeguard personal data. You should ensure you are familiar with and follow our security policies and procedures, which are designed to protect our IT systems, our premises and data within them (both confidential information and personal data).

You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality: only people who have a need to know and are authorised to use the personal data can access it;
- Integrity: personal data is accurate and suitable for the purpose for which it is processed; and
- Availability: authorised users are able to access the personal data when they need it for authorised purposes.

Passwords

In particular, both BMI employees and Contractors are responsible for safeguarding Personal data by using password protection. 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. Passwords should also be changed with regularity or when deemed necessary by IT.

Data sharing

Personal data cannot be shared with any third party or any organisation (including other BMI group companies and to our service providers) unless appropriate Data Processing Agreements and standard data protection clauses as the case may be have been put in place or the disclosure is otherwise permitted under data protection law.

If you need to share personal data outside of our organisation, you must first verify that appropriate Data Processing Agreements and standard data protection clauses are in place. This can be checked by emailing Compliance@BMIGroup.com.

Before contracting with any third party providers which should process Personal Data on BMI's behalf, we must first carry out security due diligence to verify that they meet our data protection standards for personal data and are compliant with the GDPR. Please refer requests for due diligence assistance to grc@bmigroup.com.

BMI will only contract with vendors that provide sufficient guarantees regarding the implementation of appropriate technical and organisational measures and ensure the protection of the individuals' 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 individuals and the obligations and rights of BMI.

9. Purpose limitation and data minimisation

When collecting Personal data, Employees and Contractors should be careful not to collect excessive Personal data. This means that the only personal data that should be collected is that which is necessary to achieve the purpose for which we collected it. For example, if an individual wishes to subscribe to our marketing lists, collecting their name, email address and employer name are likely to be necessary categories of data. However, it would not be necessary to collect their home telephone number or date of birth.

10. Accuracy

BMI must take reasonable efforts to ensure the Personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Employees and Contractors must check the accuracy of any Personal data at the point of collection and at regular intervals afterwards. For example, when contacting business partners for the first time in a long period, it is good practice to check if their details are still accurate. BMI must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

11. Rights of Individuals

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

GDPR rights are as follows:

- **Right to access:** Individuals 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 individual directly, and to whom the data has been disclosed, if applicable.

  Individuals also have the right to obtain from BMI a copy, free of charge, of all the Personal data BMI holds about them.

- **Right to erasure:** Individuals have the right to request 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.

  This is not an absolute right, and BMI may refuse if 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 defence of legal claims.

- **Right to rectification:** Individuals have the right to obtain from BMI rectification of their Personal data. BMI must make reasonable efforts to keep personal data in its possession or control accurate, complete, current and relevant.
- **Right to restriction:** Individuals 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 individuals require the same for the establishment, exercise or defence of legal claims, or if
  - they object to the data's processing while BMI verifies whether BMI's legitimate grounds override theirs.

- **Right to portability:** At the individual's request and where technically feasible, BMI must transfer their Personal data to another Controller, specified by the individual, provided that the processing is based on the individual's consent or necessary for the performance of a contract.

- **Right to object:** Individuals 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 based on BMI's legitimate interests. They can also object to direct privacy marketing at any time.

If you receive an individual rights request, please contact Privacy@BMIGroup.com. Bear in mind it doesn't have to mention GDPR or state it is a rights request. You could merely receive an email asking for a copy of all information BMI holds about the requester.

12. Personal Data Breaches/ Notification Obligations

If you believe that there has been a personal data breach, please contact Compliance@BMIGroup.com as soon as possible. Avoid using the term "data breach" as this may affect BMI's reporting obligations, instead refer to the event as a potential personal data event or incident.

Common examples of a data incident include (but are not limited to):

- Leaving a laptop on the train/bus.
- Clicking on a 'phishing' email.
- Sending a list of employees to an unauthorised supplier or vendor.
- Leaving a copy of a colleague's medical records on the printer, where other employees may be able to access/view those records.

Following notification of a potential security incident, BMI will follow its data incident response protocol. This may involve notifying the relevant data protection authority or the affected individuals, in accordance with the timescales set out in the GDPR.

13. Special Categories of Personal Data

The processing of special category Personal data is subject to further GDPR requirements. It must be handled with care and subject to additional security measures. Employees will have limited and restricted access to this data for specific purposes. For example, your annual training records are only visible to those HR and leadership members that need to have access to the same. It must not be moved or copied (without the explicit written instruction of the Legal Department).

BMI cannot 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. International transfers of personal data

The GDPR restricts data transfers to countries outside the UK/EU to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Personal data is transferred when personal data originating in one country is transmitted, sent, viewed or accessed in or to a different country outside the EU or UK as the case might be. Be cautious in emailing or providing remote access to any Personal data to recipients outside your organisation. Please contact Privacy@BMIGroup.com for further information.

15. Record-keeping

The GDPR requires us to keep full and accurate records of all our data processing activities. If any of the processing activities change or a new processing activity is created, please contact your region or country's in-house legal counsel so that they may update our records.

16. Privacy by design and DPIAs

BMI must consider and "bake in" privacy whenever planning or undertaking data processing. It also means that by default we selected the most privacy-friendly option.

BMI must assess what privacy by design measures can be implemented on all programmes, systems or processes that process personal data by taking into account the following:

- The state of the art.
- The cost of implementation.
- The nature, scope, context and purposes of processing.

- The risks of varying likelihood and severity for rights and freedoms of the individual posed by the processing.

In the event of high-risk processing, BMI must conduct a DPIA.

What is high risk depends on the circumstances. You should conduct a DPIA by contacting Privacy@BMIGroup.com and discuss your findings with the Legal and Compliance Team when implementing major system or business change programs involving the processing of personal data including:

- Use of new technologies (programmes, systems or processes), or changing technologies (programmes, systems or processes) e.g. machine learning.
- Automated processing including profiling and automated decision-making.
- Large-scale processing of special category personal data.
- Large-scale, systematic monitoring of a publicly accessible area e.g. using a drone to inspect a roof.

17. Training

BMI is required to ensure its Employees understand and are aware of the requirements of data protection law.

Employees are expected to participate in and complete any training assigned to them. Employees may also be required to attain a certain score of level within the training, and may be required to repeat the training or undergo additional training.

18. 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. 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.

19. Contact

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

Privacy@BMIGroup.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 can also contact the data protection officer directly by writing an email to Privacy@BMIGroup.com.