BM GREENTECH BERHAD AND GROUP OF COMPANIES

PERSONAL DATA PROTECTION (“PDP”) POLICY

Version 1: Effective 27th August 2025

CONTENTS **PAGE**

[This page is intentionally left blank]

1. Introduction

BM GreenTech Berhad and its subsidiaries ("**Group**") are committed to upholding the highest standards of personal data protection as provided for in the Malaysian Personal Data Protection Act 2010 ("**PDPA**") and any amendments made thereto.

In compliance with the PDPA and its related regulations, including any applicable orders, codes of practice, policies, standards or guidelines, the publication of this Personal Data Protection Policy **("Policy")** on the Group's website, applications and other official platforms shall serve as a Notice to all our valued clients and prospective clients.

This Policy informs you of your rights concerning your personal data that has been and/or will be collected and processed by us.

2. Personal Data Protection Principles

Pursuant to Section 5 of the PDPA, a Data Controller shall comply with the following seven (7) Personal Data Protection Principles in order to maintain the integrity of personal data:

(a) General Principle – This principle prohibits the Data Controller from processing a Data Subject's personal data without consent unless such processing is necessary. Processing of Sensitive Personal Data (as defined herein) requires explicit consent of the Data Subject;

(b) Notice and Choice Principle - This principle compels the Data Controller to inform the Data Subject by written notice as to the type, purpose, extent, accuracy and consequences of the personal data being processed;

(c) Disclosure Principle – This principle prohibits the disclosure of personal data without the consent of the Data Subject except in certain circumstances, such as instances where the disclosure is authorized by an Order of a Court or requested by law enforcement authorities;

(d) Security Principle - This principle imposes a duty on Data Controllers to take reasonable and practical steps to safeguard personal data from loss, misuse, unauthorized or accidental access, disclosure, alteration or destruction. This includes implementing appropriate security measures to safeguard the personal data;

(e) Retention Principle - This principle prohibits the Data Controllers to retain Data Subject's personal data longer than necessary for the fulfilment of the purpose for which it was collected and processed. Once the data is no longer required, it must be securely disposed or anonymized in accordance with best practices.

(f) Data Integrity Principle - This principle requires the Data Controller to take reasonable steps to ensure that personal data is accurate, complete, not misleading, and kept up to date. These obligations must be fulfilled with reference to the purpose for which the data was originally collected and processed.

(g) Access Principle – This principle grants Data Subjects right to access their own personal data and to request corrections to any data that is inaccurate, incomplete, misleading, or outdated. However, this right is subject to certain exceptions as outlined in Section 32 of the PDPA where the Data Controller may refuse to comply with the Data Subject request.

3. Interpretation

Biometric Data	Any personal data resulting from technical processing relating to the physical, physiological or behavioral characteristics of a person.
Commissioner	The Personal Data Protection Commissioner is an agency under the Digital Ministry that was created on 15 November 2013 after Parliament passed the Bill relating to the Personal Data Protection Act 2010 (PDPA).
Commercial transaction	Any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, and agency but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.
Data Controller	A person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data but does not include a Data Processor.
Data Subject	An individual who is the subject of the personal data and shall not include a deceased individual.
Data Processor	Any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user and does not process the personal data for any of his/her own purposes.
Personal Data	Any information in respect of commercial transactions, which: (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a Data Subject, who is identified or identifiable from that information or from that and other information.

3. Interpretation (Cont'd)

Processing	Collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including: (a) the organization, adaptation or alteration of personal data; (b) the retrieval, consultation or use of personal data; (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of personal data
Personal Data Breach	Any incident involving the breach, loss, misuse or unauthorized access of personal data.
Sensitive Personal Data	Any personal data consisting of information as to the physical or mental health or condition of a data subject, his/her political opinions, his/her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by his/her of any offence or any other personal data as the Minister may determine by order published in the Gazette.
Third Party	Any person other than: (a) a data subject; (b) a relevant person in relation to a data subject; (c) a data user; (d) a data processor; or (e) a person authorized in writing by the data user to process the personal data under the direct control of the data user.
Relevant Person	(a) in the case of a data subject who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the data subject; (b) in the case of a data subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorized in writing by the data subject to act on behalf of the data subject; or (c) in any other case, a person authorized in writing by the data subject to make a data access request, data correction request, or both such requests, on behalf of the data subject.

4. Why Do We Collect Your Personal Data

The Group is committed to providing you with the best possible experience as our valued customer. To support this commitment, we collect and use your personal data either directly from you or through authorized parties acting on your behalf (third party) for purposes including but not limited to, the following:

(a) Delivering enhanced products and services tailored to your needs;

(b) Managing subscriptions to newsletters or promotional items;

(c) Maintaining internal records and conducting marketing and advertising activities;

(d) Ensuring compliance with applicable legal and regulatory requirements;

(e) Facilitating effective communication with you regarding our products and services;

(f) Enabling your participation in contests, events or activities organized by us; and

(g) Processing payments related to the services you request.

5. What Personal Data Do We Collect

Depending on the nature of your interaction with the Group, we may collect various types of personal data for the purpose of facilitating commercial transactions and providing our products or services. This may include but is not limited to the following:

(a) Personally identifiable information such as your full name, age, gender, identity card number or passport, nationality and religion;

(b) Contact information, including billing address, mobile phone number, email and Internet Protocol (IP) address;

(c) Payment information, such as debit or credit card details (including cardholder name, card number, billing address, expiry date) and other bank account information;

(d) If permitted by law, sensitive information, including racial or ethnic origin, political opinions, religious beliefs, health information, biometric data or criminal background;

(e) Photographic images recorded at and around our offices, convenience stores or branches captured via closed-circuit television (CCTV) and/or screen-based visitor management systems or other devices;

(f) Photographs taken during our corporate events or other functions;

(g) Information from audio or visual recordings of calls;

(h) Information from resumes or CVs submitted when applying for employment with us.

6. When Do We Collect Your Personal Data

The Group may collect your personal data in physical (hard copy), digital or verbal form through various channels, including but not limited to:

(a) Face-to-face interactions at our stores, offices or other premises;

(b) Application forms, registration documents, and business cards;

(c) Communications such as via email, phone calls, SMS or messaging platforms (e.g., WhatsApp);

(d) Your use of our websites, mobile applications or other online services;

(e) Interactions with us on social media platforms;

(f) When you access our websites or mobile applications through automated technologies such as cookies, web beacons and other online tracking tools;

(g) When we capture photographic images recorded at our premises for security and safety purposes via closed-circuit television (CCTV) and/or screen-based visitor management systems or other devices;

(h) When we receive information from third parties acting on your behalf including agents, service providers or business partners; and

(i) When we receive information provided in application forms for processing purposes such as supplier registration or onboarding of business associates.

7. How Do We Use Your Personal Data

Your personal data may be used by the Group in the course of conducting our business operations and activities, including but not limited to the following purposes:

(a) Employment Related Purposes

We may use your personal data to support employment-related processes such as recruitment, onboarding, payroll, performance management, training, compliance with employment laws and other human resource functions. This includes data provided by job applicants, employees, and interns for operational, regulatory purposes or third-party service providers engaged to support our human resource functions, in accordance with applicable laws and internal policies.

(b) Consumer Service

We may use your personal data to respond to enquiries and provide customer support. This typically includes using your contact details and relevant information related to your inquiry (e.g., order status, technical issues, product complaints, or general questions).

7. How Do We Use Your Personal Data (Cont'd)

(c) Contests, Marketing and Promotions

We may use your personal data to inform you about our products, services, promotions, campaigns, and contests. Communications may occur via email, SMS, phone calls, instant messaging (e.g., WhatsApp), online advertisements, or postal mail, in accordance with applicable laws.

We may also use or disclose your personal data including your name, contact details, NRIC number and photographs or videos for identification and promotional purposes when you participate in our on-ground events or contests. Certain campaigns may be hosted on third-party platforms or social media. Participation in such activities is voluntary, and you may opt out or withdraw your consent at any time.

(d) Personalization

We may use your personal data to analyze preferences and behaviors, anticipate your needs, enhance and personalize your experience on our websites or mobile apps, optimize content, deliver targeted advertisements, and enable interactive features you choose to use.

(e) Order Fulfilment

We may use your personal data to process and deliver your orders, verify your identity, confirm delivery information and detect or prevent fraud. Communications related to your orders may be made through various channels, including but not limited to email, SMS, phone calls, postal mail or messaging applications such as WhatsApp.

(f) General Business Purposes

We may use your personal data for internal purposes such as maintaining customer accounts, conducting market research, improving customer experience, or evaluating the effectiveness of our marketing campaigns.

8. To Whom Do We Disclose Your Personal Data

In the course of providing our services to you, we may be required to disclose your personal data to the following third parties, among others:

(a) Group affiliated companies;

(b) Federal or State bodies

(c) Government bodies and law enforcement agencies/authorities;

(d) Regulatory authorities;

(e) Companies or organizations acting as our service providers, agents, contractors, business partners, banks and financial institutions;

8. To Whom Do We Disclose Your Personal Data (Cont'd)

(f) Professional firms, advisers or consultants;

(g) Other parties to whom you have given your express or implied consent;

(h) Credit reporting or debt collecting agencies (in the event of payment default), as permitted under the applicable laws; or

(i) Any other party deem fit and proper by the Group.

9. How Do We Safeguard Your Personal Data

We are committed to safeguarding your personal data and strive to implement appropriate physical, technical and procedural measures to reduce the risk of accidental loss, unauthorized access, misuse, alteration or disclosure.

As such, personal data provided through our website, applications or other platforms are protected during transmission using encryption technologies such as Transport Layer Security (TLS). Within our organization, access to stored personal data is strictly limited to authorized personnel only and managed through secure computer systems located in facilities with robust physical security measures. Meanwhile, data stored in cloud environments, including third-party services is also encrypted to ensure confidentiality. Additionally, we apply equally stringent procedures and security controls to safeguard personal data maintained in non-electronic formats.

Our approach to data protection includes but not limited to the following practices:

(a) Employees must be registered in an internal system before being granted access to personal data;

(b) Access rights are promptly revoked when employees resign, their contracts end or their roles change;

(c) Access to personal data systems is strictly controlled and limited based on job responsibilities;

(d) Only authorized employees are assigned unique user IDs and passwords to access personal data;

(e) User IDs and passwords are immediately deactivated when employees no longer handle personal data;

(f) Physical security measures include:

- Controlled entry and exit points at data storage areas;
- Secure storage of personal data in protected locations;
- Installation of CCTV cameras at storage sites where necessary;
- 24-hour security surveillance (where applicable).

9. How Do We Safeguard Your Personal Data (Cont'd)

(g) Technical safeguard measures include:

- Antivirus software is implemented and regularly updated to help protect against security threats and minimize the risk of data breaches;
- Computer systems are protected against malware and cyber threats to safeguard personal data;
- Access to personal data is regularly monitored and documented, and records are made available to the Personal Data Protection Commissioner upon request

(h) All third-party processors engaged by us are required to comply with the Security Principles under the PDPA, implement appropriate technical and organizational measures to safeguard personal data and enter into binding agreements that ensure the proper handling and protection of personal data in compliance with applicable laws and our internal policies.

(i) Once your personal data is no longer necessary for the purposes of which it was collected, we will ensure its secure deletion in accordance with the General Code of Practice for Personal Data Protection.

10. Use of Cookies

Our website, applications and other platforms use cookies which are stored by our servers to recognize the user or user's device during each visit. These cookies are associated with anonymous users and do not contain or collect any personal data that can identify you.

Some cookies may also be placed by authorized third parties to help us assess the effectiveness of our engagements, promotions and marketing activities. These third-party cookies likewise do not collect personal data that identifies specific individuals.

These cookies are temporary in nature and are used solely to enhance the efficiency of the user's browsing experience. You may configure your browser settings to notify you when cookies are being used and to prevent their installation on your computer or smart device.

11. Cross Border Personal Data Transfer

Your personal data may be transferred between countries, provided always that:

(a) Your consent has been obtained;

(b) The transfer is necessary for the performance of a contract between us and a third party;

(c) The transfer is necessary for the purpose of legal proceedings, obtaining legal advice, or defending legal rights;

(d) The transfer is for the avoidance or mitigation of adverse action against you;

(e) The transfer is necessary to protect your vital interests; or

(f) We have taken all reasonable precautions and exercised due diligence to ensure that personal data processed in the destination country is subject to adequate protection standards and will not be handled in any manner that contravenes the PDPA.

12. Data Subject Obligation

You are responsible for providing accurate, complete, and non-misleading personal data to us, and for ensuring that such data is kept up to date, taking into account the purposes for which it is collected and processed. Failure to provide the required personal data may, among others:

(a) result in us preventing your entry to our premises or participation in our events;

(b) result in our inability to process your application and/or provide you with our services;

(c) result in our inability to respond to your requests regarding our products or services;

(d) limit or prevent your access to certain features on our website or weblinks;

(e) result in our inability to inform you of our latest updates on promotions, services, products or launches;

(f) result in your inability to receive invitations to promotional activities organized by us, thereby affecting our ability to communicate with you;

(g) result in our inability to enter into or continue a contract with you and negatively impact your chances of being selected for potential employment, engagement or internship opportunities.

13. Data Subject Rights

Data subjects are entitled to a range of rights under the PDPA, including but not limited to the following:

(a) To request for access to personal data

- You have the right to submit a written request to access your personal data that is being processed by us, and to receive a copy of such data. We will process and respond to your request within twenty-one (21) days from the date we receive it. If we are unable to comply within this time frame, we will inform you accordingly. We may refuse to comply to your request if the information provided is insufficient as may be reasonably required.

(b) To request for correction of personal data

- You have the right to request, in writing, the correction of your personal data if you believe it is inaccurate, incomplete, misleading, or outdated. We will process and respond to your request within twenty-one (21) days from the date we receive it. If we are unable to comply within this time frame, we will inform you accordingly.
- We may decline to act on your request if the information provided is insufficient as may be reasonably required. Additionally, we will only proceed with the release or correction of your personal data upon verification and/or validation of your identity to ensure the security and accuracy of the request.

(c) To withdraw consent from processing personal data

- You have the right to submit a written request via email to us to cease processing your personal data. Upon receiving your written request, we will cease processing your personal data. Please note that withdrawing your consent may limit our ability to provide services, respond to your enquiries or maintain any ongoing business or employment relationship with you.

(d) To request for transmission of personal data to another Data Controller (Data Portability)

- You have the right to request the transmission of your personal data to another Data Controller of your choice. To exercise this right, you must submit a written request via email to us (refer to Contact Us section below), subject to the condition that the data format is technically feasible and compatible. Upon receipt of your request, we will carry out the data transfer within 21 days. In the event we are unable to comply within the 21 days period, we shall comply with your request no later than 14 days after the expiration of the initial 21 days period.

14. Personal Data of Children

We are unable to distinguish the age of users who access our Website, Mobile App or social media platforms. As a result, we may inadvertently collect and process personal data of individuals under the age of eighteen (18).

If you are under 18, please obtain consent from your parent, guardian or person with parental responsibility before providing your personal data to us. If we become aware that we have collected personal data from a child under the age of 18 without parental or guardian consent, we will take steps to delete such data. If you believe that we may have collected data from or about a child without the necessary consent, please contact us immediately.

15. Notification of Personal Data Breach

If we have reasons to believe that a personal data breach has occurred, we will notify the Commissioner and affected Data Subjects of a personal data breach, ensuring that such breaches are managed effectively and in compliance with the requirements of PDPA.

A personal data breach may be caused by accidental or deliberate actions, either internally or externally. We are required to notify the Commissioner as soon as practicable, and no later than seventy-two (72) hours after becoming aware of a personal data breach.

If the breach causes or is likely to cause significant harm, we shall notify the affected Data Subject as soon as practicable, and no later than seven (7) days after the initial notification to the Commissioner. In this context, “significant harm” refers to the risk that the compromised data:

(a) may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;

(b) may be misused for illegal purpose;

(c) consist of sensitive personal data;

(d) consist of personal data and other personal information which, when combined, could potentially enable identity fraud; or

(e) is of significant scale (if the number of affected Data Subjects exceeds one thousand).

In the event that, due to circumstances beyond our control, we are unable to notify the Commissioner within seventy-two (72) hours after becoming aware of a personal data breach, we will provide notification as soon as possible thereafter through written notice, accompanied by supporting evidence.

For avoidance of doubt, we are required to provide the following details to the Commissioner:

(a) date and time of the personal data breach detected;

(b) type of personal data involved and nature of the breach;

(c) method used to identify the breach and the suspected cause of the incident;

(d) number of affected data subjects;

(e) estimated number of affected data records;

(f) personal data system affected, which resulted in the breach;

15. Notification of Personal Data Breach (Cont'd)

(g) potential consequences arising from the personal data breach;

(h) chronology of events leading to the loss of control over personal data;

(i) measures taken or proposed to be taken by us to address the personal data breach, including steps implemented or planned to mitigate the possible adverse effects of the breach;

(j) measures taken or proposed to be taken to address the affected data subjects; and

(k) contact details of the Data Protection Officer from whom further information may be obtained.

The notification from us to the affected Data Subjects shall include the following information:

(a) details of the personal data breach that has occurred;

(b) details on the potential consequences resulting from the personal data breach;

(c) measures taken by us to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

(d) measures that the affected Data Subjects may take to eliminate or mitigate any potential adverse effects resulting from the data breach; and

(e) contact details of the Data Protection Officer from whom further information may be obtained.

16. Breach of Personal Data Protection Principles

Upon conviction, any breach of the Data Protection Principles set out in this Policy may result in a fine not exceeding Ringgit Malaysia One Million (RM1,000,000), imprisonment for a term not exceeding three (3) years or both in accordance with the PDPA.

17. Retention of Personal Data

We will process your personal data only for as long as we have a lawful basis to do so. Your personal data will be retained solely for the period necessary to fulfill the purposes outlined above, unless retention is required by other applicable laws.

At the end of the retention period, your personal data will either be permanently deleted or anonymized. For example, it may be aggregated with other data so that it can no longer be used to identify you and may instead be used for statistical analysis and business planning.

18. Acknowledgement and Consent

By communicating or engaging with us, using our products and services, browsing our corporate website, visiting our premises, attending our events (including webinars, conferences or promotional activities), interacting with our social media channels, participating in surveys or feedback, applying for employment or partnership opportunities, subscribing to our newsletters or updates or otherwise providing personal data through any digital or physical channel, you acknowledge that you have read and understood this Policy and you consent to the collection, use, processing, disclosure and transmission of your personal data as described herein.

19. Contact Us

Should you require further information about the personal data we hold, how your information is collected or used, or our compliance with this Policy, kindly contact or write to us at:

Person in Charge	:	Data Protection Officer (DPO)
Contact Number	:	03-8023 9137
Email	:	privacy@boilermech.com
Business Address	:	Lot 873 & 875, Jalan Subang 8, Taman Perindustrian Subang, 47620 Subang Jaya, Selangor Darul Ehsan

20. Review of Policy

We reserve the right to update or amend this Policy at any time without prior notice. We encourage you to regularly visit our website at www.boilermech.com.my to stay updated on any changes to this Policy.