Attachment No. 9

Data Protection Policy
(In accordance with the Personal Data Protection Act B.E. 2562)

Millennium Group Corporation (Asia) Public Company Limited ("the Company") recognizes the importance of personal data protection and operates in compliance with the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws, including ministerial regulations and related announcements that may come into effect in the future, to the extent that they are applicable to the Company's operations (collectively referred to as the "Personal Data Protection Laws").

Accordingly, the Group Chief Executive Officer deems it appropriate to enforce this Personal Data Protection Policy within the Company and its subsidiaries in order to establish guidelines for governance and management of personal data to ensure that the collection, use, or disclosure of personal data by the Company and its subsidiaries is protected in accordance with the Personal Data Protection Laws. The key principles of the Personal Data Protection Policy are as follows:

1. Directors, executives, employees, permanent staff, and temporary staff of the Company or its subsidiaries must strictly comply with applicable laws, policies, regulations, rules, manuals, or guidelines of the Company relating to personal data protection.
2. Directors and executives in all departments must promote awareness among employees, permanent staff, and temporary staff of the Company or its subsidiaries regarding the importance of personal data protection and encourage personal data protection risk management at all levels of the organization, including implementing effective internal control measures to prevent unlawful collection, use, or disclosure of personal data.
3. The Company shall appoint the Head of Personal Data Protection Unit (Head of PRC), who shall act as the Data Protection Officer (DPO) under the Personal Data Protection Act B.E. 2562 (2019), to provide advice, consultation, and oversight on activities related to the collection, use, or disclosure of personal data by the Company or its subsidiaries in compliance with the Personal Data Protection Laws. The Head of PRC shall also coordinate and cooperate with the Office of the Personal Data Protection Committee. Directors and executives of the Company or its subsidiaries must support the performance of duties of the Head of PRC by providing adequate tools, resources, and facilitating appropriate access to personal data necessary for the performance of such duties.
4. Personal data shall be collected only to the extent necessary and for lawful purposes related to the processing of personal data by the Company or its subsidiaries.
5. The collection, use, or disclosure of personal data must have a lawful basis. Where consent is required by law, explicit consent from the data subject must be obtained. The Company must also inform the data subject of the necessary details prior to or at the time of collection of personal data as required by law.

6. The collection, use, or disclosure of personal data must be carried out in accordance with the purposes notified to the data subject prior to or at the time of collection, unless otherwise permitted by law. In cases where personal data is collected from sources other than the data subject directly, the Company or its subsidiaries must notify the data subject without delay and obtain consent where required by law, unless an exemption under the Personal Data Protection Laws applies.
7. The Company shall require all internal departments and subsidiaries to prepare and maintain records of processing activities (Record of Processing Activities: ROPA) in accordance with the criteria and procedures prescribed by law, enabling data subjects and the Office of the Personal Data Protection Committee to verify such records. These records must be accurate, complete, and kept up to date at all times.
8. The Company and its subsidiaries must implement appropriate security measures to protect personal data against loss, unauthorized access, use, alteration, or disclosure. Such measures must be regularly reviewed and assessed, or whenever necessary or when technological changes occur, to ensure that personal data protection measures remain effective, adequate, and compliant with legal requirements.
9. The Company and its subsidiaries must implement systems for monitoring and managing personal data to ensure that personal data is erased, destroyed, or anonymized once it is no longer necessary for the purposes for which it was collected, unless retention is required by law.
10. Where the Company or its subsidiaries engage a data processor to process personal data on their behalf, the Company or its subsidiaries must establish an agreement with such processor to ensure that the processing activities comply with the Personal Data Protection Laws and prevent unauthorized use or disclosure of personal data. The Company must also implement monitoring and auditing mechanisms to regularly review the performance of the data processor to ensure strict compliance with the agreement and applicable laws.
11. In cases where personal data is disclosed to external organizations or individuals upon request for access to personal data held by the Company or its subsidiaries, such as government authorities, regulatory bodies, officials exercising legal powers, or insurance companies, the Company or its subsidiaries must ensure that such disclosure has a lawful basis. Where consent is required by law, consent must be obtained from the data subject unless an exemption applies, such as compliance with legal obligations, protection of life, body, or health, or necessity for establishing legal claims. The Company or its subsidiaries must maintain a record of such disclosures.
12. Where it is necessary for the Company or its subsidiaries to transfer personal data to foreign countries, the Company or its subsidiaries must ensure that the destination country has adequate personal data protection standards or that appropriate safeguards are in place, such as a Data Transfer Agreement or other mechanisms prescribed by law.
13. Directors, executives, employees, permanent staff, temporary staff, and contractors of the Company or its subsidiaries must notify any personal data breach to the Office of the Personal Data Protection Committee within 72 hours or within the period prescribed by law after becoming aware

of the breach. The Company must also notify the affected data subjects without delay if the breach is likely to result in a high risk to the rights and freedoms of the data subjects, unless the breach is unlikely to pose such risk.

14. Directors, executives, employees, permanent staff, temporary staff, and contractors of the Company or its subsidiaries must cooperate with the Head of Personal Data Protection Unit and the Office of the Personal Data Protection Committee when requested to provide documents or information related to personal data protection, including clarifying facts to support investigations and compliance with the Personal Data Protection Laws.
15. The Company shall provide regular training and education on personal data protection to employees at all levels in order to raise awareness and strengthen knowledge regarding compliance with the Personal Data Protection Laws.