MC GROUP

Personal Data Protection Policy

Mc Group Public Company Limited

Effective from February 11, 2021

Mc Group Public Company Limited

Personal Data Protection Policy

Mc Group Public Company Limited recognizes and emphasizes the importance of protecting the personal data of customers, shareholders, partners, and employees. Therefore, this personal data protection policy has been established to serve as a guideline, including the definition of criteria and measures for the appropriate and clear protection of personal data, ensuring the rights of data owners as stipulated by the Personal Data Protection Act, as well as the various regulations set forth by government agencies overseeing this matter. The Board of Directors of Mc Group Public Company Limited approved this policy at the meeting No. 1/2021 on February 11, 2021.

1. Scope of Application

1.1 This personal data protection policy is applicable to directors, advisors, executives, auditors, and employees of the company, including partners, customers, and any other individuals or legal entities bound by a contract with the company.

1.2 This personal data protection policy is applicable to all operations of the company related to the processing of personal data.

2. Definitions

The terms and definitions used in this Personal Data Protection Policy shall have the following meanings:

2.1 **"Company"** refers to Mc Group Public Company Limited and its subsidiaries.

2.2 **"Subsidiary"** refers to a limited company or a public limited company that is under the control of Mc Group Public Company Limited, in accordance with the criteria defined by the Securities and Exchange Commission.

2.3 **"Personal Data"** means information related to an identifiable natural person, such as name, surname, address, phone number, date of birth, gender, email, national ID number, or other data that can identify the individual, either directly or indirectly.

2.4 **"Data Subject"** means a natural person whose personal data can be identified, either directly or indirectly.

2.5 **"Data Controller"** refers to a natural person or legal entity with the authority to make decisions regarding the processing of personal data.

2.6 **"Data Processor"** refers to a natural person or legal entity that processes personal data on behalf of or under the instructions of the Data Controller.

2.7 **"Data Processing"** refers to any action taken with personal data, such as collection, recording, organization, structuring, storage, modification, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, merging, deletion, or destruction.

3. **Purposes of Collecting, Using, and Disclosing Personal Data**

The Company may collect, use, and disclose personal data of the data subjects for the following purposes:

3.1 To enter into or perform contractual obligations between the Company and the data subject, or to perform contractual obligations between the Company and third parties for the benefit of the data subject.

3.2 To respond to inquiries and provide assistance to the data subject.

3.3 To develop and improve the Company's goods, products, and services to better meet the needs of the data subject.

3.4 To provide information and recommendations regarding goods, products, services, or marketing promotions, promotional campaigns, or benefits through the contact channels provided by the data subject.

3.5 To conduct surveys, analysis, research, and prepare statistical data for marketing purposes or to develop and improve the Company's operations.

3.6 For the benefit of internal management or operations of the Company, as required under legitimate interests.

3.7 To audit, supervise, and maintain security at the Company's buildings or premises.

3.8 To comply with laws related to the Company's operations, such as withholding tax obligations.

3.9 To provide information to government agencies with legal authority, as requested by such agencies, such as the Royal Thai Police, the Anti-Money Laundering Office, the Revenue Department, and the courts.

4. Collection of Personal Data

4.1 Sources of Personal Data

The Company may obtain personal data of data subjects from the following sources:

4.1.1 Collected directly from the data subject, such as through forms filled out by the data subject in either paper or electronic format.

4.1.2 Collected from other sources, such as from third parties under the consent provided by the data subject to the disclosing party, or from data processors acting on behalf of or under the Company's instructions.

4.2 Types of Personal Data Collected

4.2.1 Personal identifiers, such as name, surname, date of birth, nationality, national ID number, or any other identification document issued by government authorities.

4.2.2 Contact information, such as address, email, and phone number.

4.2.3 Information related to website usage, such as username, password, IP address, and cookie data.

4.2.4 Sensitive data, such as religion, health information, and criminal records.

4.2.5 Other personal data, such as voice recordings, photographs, CCTV footage, and fingerprints.

4.3 Criteria for Collecting Personal Data

The Company will collect only the necessary personal data for the purposes communicated to the data subject. The Company will obtain explicit consent from the data subject before or at the time of data collection, except in the following cases where the Company may collect personal data without consent:

4.3.1 To achieve objectives related to public interest archives, historical documentation, research, or statistical purposes, provided that the Company implements appropriate measures to protect the rights and freedoms of the data subject.

4.3.2 To prevent or suppress danger to life, body, or health of an individual.

4.3.3 When it is necessary for the performance of a contract to which the data subject is a party, or to process the data subject's request prior to entering into a contract.

4.3.4 When it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company.

4.3.5 When it is necessary for the legitimate interests of the Company or another person or legal entity, unless such interests are overridden by the fundamental rights and freedoms of the data subject.

4.3.6 To comply with legal obligations, such as the Credit Information Business Act of 2016, the Civil and Commercial Code, or the Criminal Code.

5. Use and Disclosure of Personal Data

The Company may use and disclose the personal data of data subjects for the purposes stated in Section 3. The Company may disclose personal data to external entities or individuals only to the extent necessary and with the consent of the data subject, or as permitted by law. Recipients of such personal data will collect, use, and/or disclose personal data only within the scope of the consent provided by the data subject, the relevant provisions of this policy, or as required by law.

Personal data of data subjects may be disclosed to the following entities or individuals:

5.1 Mc Group Public Company Limited and its subsidiaries, including directors, executives, advisors, and employees of the Company.

5.2 The Company's contractual partners, service providers, and business partners who have a relationship or agreement with the Company.

5.3 Auditors.

5.4 Government agencies with legal authority, such as the Anti-Money Laundering Office, the Royal Thai Police, the Revenue Department, the Legal Execution Department, and the courts.

5.5 Other entities or organizations related to the Company's business operations, such as banks, financial institutions, insurers, and hospitals.

6. Duration of Personal Data Collection, Use, and Disclosure

The Company will collect, use, and disclose personal data of data subjects for the necessary period while the data subject remains a customer, partner, employee, or maintains a relationship with the Company. The retention period will depend on the necessity and appropriateness for each type of personal data. In some cases, the Company may be required to retain the data beyond this period as mandated or permitted by law, such as for compliance with tax laws, anti-money laundering laws, securities and exchange laws, or within the statutory limitation period not exceeding 10 years.

The Company will delete, destroy, or anonymize personal data when it is no longer necessary or after the retention period has ended.

7. Rights of Personal Data Subjects

Data subjects have the following rights as stipulated by law:

7.1 The right to access, obtain a copy, or request the disclosure of the source of their personal data.

7.2 The right to request the transfer of their personal data.

7.3 The right to request correction, addition, or modification to ensure their personal data is accurate, complete, and up-to-date.

7.4 The right to object to the collection, use, or disclosure of their personal data at any time.

7.5 The right to request the suspension of the use of their personal data.

7.6 The right to request the deletion, destruction, or anonymization of their personal data.

7.7 The right to withdraw consent to the collection, use, or disclosure of their personal data.

These rights must be exercised according to the procedures and conditions set by the Company. However, the Company may refuse the request of the data subject within the limits permitted by law.

8. Personal Data Security Measures

The Company has established standard security measures in both technology and practices to control and prevent loss, leakage, theft, unauthorized access, use, modification, alteration, disclosure, destruction, and transfer of personal data, contrary to the law's provisions, as follows:

8.1 The Company sets permissions for accessing, using, disclosing, and processing personal data, including identity verification for individuals who access, use, or process personal data.

8.2 The Company maintains a record of personal data processing (Records of Processing) to document the activities related to personal data processing.

8.3 If the Company, as a data controller, outsources data processing to an external party (the data processor), the Company will require the signing of a data processing contract to define the scope, objectives, duties, and responsibilities concerning personal data protection, ensuring compliance with this policy and legal requirements.

8.4 When transferring or transmitting personal data abroad, including storing personal data on databases in other systems, the destination country or system where the data is stored must have personal data protection measures equal to or better than those outlined in this policy.

8.5 In the event of a breach of the Company's security measures resulting in personal data violation or leakage into the public domain, the Company will promptly inform the data subject and provide a damage recovery plan for the violation or leakage caused by the Company's negligence. The Company will not be responsible for any damages arising from the use or disclosure of personal data to third parties, including failure or neglect to log out from databases or social media systems by the data subject or by persons authorized by the data subject.

8.6 The Company conducts regular reviews and assessments of the effectiveness of personal data security systems by the internal audit department.

9. Data Protection Officer

The Company has complied with the Personal Data Protection Act B.E. 2562 by appointing a Data Protection Officer (DPO) and establishing departments responsible for monitoring and overseeing the Company's operations in accordance with this policy and legal requirements, which include the following departments:

9.1 Information Technology Department

9.2 Legal Department

9.3 Internal Audit Department

10. Penalties

Any individual who neglects or fails to comply with, or engages in any action that violates this personal data protection policy, including related practices and legal provisions regarding personal data protection, may be subject to disciplinary action according to the Company's work regulations or as deemed appropriate by the Company. This includes potential legal action or penalties as specified by law.

11. Policy Review

The Company may review or amend this personal data protection policy as necessary to ensure compliance with relevant legal provisions and to improve practical implementation.

12. Contact Information

Data Protection Officer (Data Protection Office)
Mc Group Public Company Limited
No. 448, 450, Prawet, Prawet District, Bangkok 10250
Phone: 0 2117 9999
Email: dpo@mcgroupnet.com

13. Effective Date

This policy shall come into effect from February 11, 2021, onwards.

-Signed by-

(Mrs. Kaisri Nuengsigkapian)
Chairman of the Board of Directors