



PERSONAL DATA PROTECTION POLICY

Moshi Moshi Retail Corporation Public Company Limited

Latest Effective Edition

Original Edition, Effective July 6, 2022

Reviewed by the Board of Directors on December 23, 2025



PERSONAL DATA PROTECTION POLICY

Moshi Moshi Retail Corporation Public Company Limited

Moshi Moshi Retail Corporation Public Company Limited (“**The Company**”) collects, uses, and discloses the personal data of customers, suppliers, employees, applicants, personnel, and any other individuals associated with The Company. Fully respecting and recognizing the significance of the Personal Data Protection Act B.E. 2562 (2019), The Company has established this Personal Data Protection Policy to implement appropriate criteria, regulations, administrative frameworks, and security measures governing personal data processing. This policy shall be binding upon all employees, ensuring that all personal data received by The Company is utilized strictly in accordance with operational regulations and personal data protection legislation, as detailed below:

1. Definitions

“ The Company ”	Means Moshi Moshi Retail Corporation Public Company Limited.
“ Personal Data ”	Means information relating to a person which enables the identification of such person, whether directly or indirectly, but not including information of the deceased in particular.
“ Sensitive Personal Data ”	Means personal data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or any other data which similarly affects the data subject as prescribed by the Personal Data Protection Committee.
“ Data Controller ”	Means a person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of personal data.
“ Data Processor ”	Means a person or a juristic person who operates in relation to the collection, use, or disclosure of personal data pursuant to the orders given by or on behalf of a Data Controller.
“ Data Subject ”	Means a natural person to whom the personal data refers.
“ Data Processing ”	Means any operation concerning the collection, use, and disclosure of personal data.
“ Board of Directors ”	Means the directors of Moshi Moshi Retail Corporation Public Company Limited.
“ Executive ”	Means the executives of Moshi Moshi Retail Corporation Public Company Limited.
“ Employee ”	Means employees below the executive level of Moshi Moshi Retail Corporation Public Company Limited.
“ Privacy Notice ”	Means a notice published on the website to inform website visitors of the website's purposes, methods of collection, processing, and storage of personal data.

“Cookies”	Means unique files created by a website and stored on a user's computer or communication device, which store personal data, usage data, and various preferences of the user to improve their website experience.
-----------	--

2. Principles and Practices on Personal Data Protection

Personal Data Protection

As a Data Controller under the Personal Data Protection Act, The Company operates in accordance with the personal data protection principles outlined below. To ensure the proper use of personal data, The Company shall manage operations to comply with the following:

(1) Collection, Use, or Disclosure of Personal Data

The Company shall establish methods or formats for obtaining consent from the Data Subject, ensuring it is requested explicitly and without complexity, either in writing or via an electronic system.

(2) Notification of Purposes for Collection, Use, or Disclosure of Personal Data

The Company shall establish methods or formats to clearly notify the Data Subject of the purposes and necessary information prior to or at the time of collection, either in writing or via an electronic system (provided that The Company limits the collection of personal data to what is strictly necessary for the purposes notified to the Data Subject).

(3) Safeguarding Personal Data

The Company shall implement security measures for the collection, use, or disclosure of personal data, including its transmission or transfer to third parties, and shall regularly review such measures to align with technological shifts, preventing unauthorized use or disclosure.

(4) Personal Data Management

- a. The Company shall define access rights and restrictions regarding personal data. Any rectification, modification, erasure, or destruction of data must be executed upon the request of the Data Subject; where The Company deems any rectification or modification appropriate, it shall notify the Data Subject on every occasion.
- b. The Company shall require monitoring and auditing of the erasure or destruction of personal data once the retention period expires, or where the data becomes irrelevant or exceeds what is necessary for the specified purposes, or upon the request or withdrawal of consent by the Data Subject.
- c. The Company shall mandate the maintenance of personal data processing records to enable access and verification by the Data Subject.
- d. The Company shall establish a process to immediately notify the Personal Data Protection Officer and the Data Subject of any personal data breaches upon detection.

-TRANSLATION-

Furthermore, where The Company obtains personal data from another data controller under a binding contractual agreement, The Company shall act as a Data Processor under the Personal Data Protection Act. To ensure the proper use of personal data, The Company shall manage operations to comply with the following principles:

(1) Collection, Use, or Disclosure of Personal Data

The Company shall operate strictly within the methods or formats designated by the Data Controller.

(2) Notification of Purposes for Collection, Use, or Disclosure of Personal Data

The Company shall operate strictly within the methods or formats designated by the Data Controller.

(3) Safeguarding Personal Data

The Company shall implement security measures for the collection, use, or disclosure of personal data, including its transmission or transfer to third parties, and shall regularly review such measures to align with technological shifts, preventing unauthorized use or disclosure.

(4) Personal Data Management

- a. The Company shall define access rights and restrictions regarding personal data. Any rectification, modification, erasure, or destruction of data must be executed strictly within the methods or formats designated by the Data Controller; where The Company deems any rectification or modification appropriate, it shall notify the Data Controller on every occasion.
- b. The Company shall require monitoring and auditing of the erasure or destruction of personal data strictly within the methods or formats designated by the Data Controller.
- c. The Company shall mandate the maintenance of personal data processing records to enable access and verification by the Data Subject, the Data Controller, and the Office of the Personal Data Protection Commission.
- d. The Company shall establish a process to immediately notify the Data Controller of any personal data breaches upon detection.

3. Purposes and Collection of Personal Data Use

3.1. As a Data Controller under the Personal Data Protection Act, The Company shall collect or use personal data for lawful and fair purposes, notifying the data subjects of such purposes to support business operations and ensure compliance with all applicable laws binding The Company or related individuals.

3.2. As a Data Controller under the Personal Data Protection Act, The Company shall collect or use personal data only to the extent necessary for operations under the specified processing purposes. Should The Company engage in any processing beyond the defined purposes, it shall notify the data subjects and obtain prior consent where required.

3.3. When collecting or using personal data, The Company shall obtain prior consent from the data subjects, unless an exemption under personal data protection legislation permits processing without such consent.

3.4. The Company shall not collect personal data regarding racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or any other data which similarly affects the data subject, unless explicit consent is obtained from the data subject or a statutory exemption applies under personal data protection laws. The Company shall collect and use such personal data with utmost care under appropriate security standards.

4. Disclosure of Personal Data

4.1. The Company may disclose personal data to individuals, government agencies, official authorities, regulatory bodies, organizations, or external juristic persons contractually bound to The Company, or as permitted under applicable legal frameworks.

4.2. The Company may disclose personal data to its affiliates to support corporate operations and benefit the data subjects, subject to appropriate security measures.

5. Personal Data Processing by Third Parties

The Company may find it necessary to transmit or transfer personal data to external parties or entities for processing. In doing so, The Company shall ensure that such transmission or transfer complies with statutory requirements, implementing necessary and appropriate safeguards aligned with confidentiality standards, such as data anonymization or pseudonymization prior to transmission, limiting data delivery to what is strictly necessary, and executing non-disclosure agreements or Data Processing Agreements with the recipients.

6. Cross-Border Transmission or Transfer of Personal Data

The Company may find it necessary to transmit or transfer personal data to affiliates within its international network or to other recipients as part of its ordinary course of business, such as storing personal data on servers or cloud platforms abroad. In such instances, The Company shall evaluate and ensure that the destination country is recognized as maintaining an adequate standard of personal data protection.

Where the destination country lacks adequate standards, The Company shall manage the transmission or transfer of personal data in strict compliance with the law, instituting personal data protection safeguards deemed necessary and appropriate under confidentiality standards. Notwithstanding an inadequate standard in the destination country, cross-border transfers remain permissible if they fall under statutory exemptions, such as legal compliance, obtaining consent from the data subject, contractual necessity, preventing or suppressing danger to life, or overriding public interest.

7. Personal Data Retention Period

The Company shall retain personal data for the duration necessary to fulfill its business objectives or as long as required to achieve the stated purposes, driving subsequent retention where mandated or permitted by law. This includes adherence to anti-money laundering legislation or preservation for evidentiary verification in potential disputes within the statutory limitation period, up to a maximum of 10 years.

Furthermore, The Company shall erase, destroy, or anonymize personal data once it is no longer necessary or upon the expiration of the aforementioned period.

8. Security Measures

8.1. The Company shall implement appropriate security measures for personal data, spanning Technical Measures (e.g., password creation, Secure Sockets Layer/SSL encryption, network security systems) and Organizational Measures (e.g., information security policies, confidentiality protocols, access control, risk assessment and management, rules and regulations). These measures shall be strictly enforced and regularly reviewed or updated alongside technological advancements to ensure robust protection, preventing personal data breaches, loss, unauthorized access, destruction, use, alteration, modification, or unlawful disclosure.

8.2. All employees and personnel of The Company are duty-bound to comply with personal data protection laws, prioritizing personal data security and refraining from utilizing work-acquired information for unauthorized purposes or causing detriment to The Company.

9. Personal Data Breaches

In the event of a personal data breach, The Company shall notify the Office of the Personal Data Protection Commission within 72 hours of becoming aware of the incident. Where the breach poses a high risk to the rights and freedoms of the data subjects, The Company shall notify the affected data subjects of the breach alongside remediation guidelines without delay.

10. Rights of the Data Subject

The rights of data subjects are statutory, enabling individuals to exercise their respective rights under legal frameworks. The Company shall process requests from data subjects without delay; should a request be denied, The Company shall inform the data subject of the grounds for such refusal.

10.1 Right to Withdraw Consent: Where a data subject has granted consent to The Company for the collection, use, or disclosure of personal data (regardless of whether such consent was provided before or after the effective date of the personal data protection law), the data subject retains the right to withdraw consent at any time throughout the retention period, unless restricted by law or an existing contract beneficial to the data subject. The Company shall inform the data subject of the potential consequences of such withdrawal.

10.2 Right to Access Personal Data: The Data Subject has the right to access or obtain a copy of their personal data under The Company's responsibility, as well as to request disclosure regarding the acquisition of data obtained without their consent. The Company reserves the right to reject a request if mandated by law or court order, or if such access or duplication would adversely affect the rights and freedoms of others.

10. 3 Right to Data Portability: The Data Subject has the right to obtain their personal data in a format that is readable or commonly usable by automated tools or devices, capable of being used or disclosed by automated means. This includes the right to request The Company to transmit or transfer the data in such format directly to another data controller where technically feasible via automated means, and to receive data transmitted directly by The Company, unless prevented by technical constraints.

Provided that the aforementioned personal data must be data for which the data subject has granted consent for collection, use, or disclosure, or data necessary for performance of a contract to which the data subject is party, or as otherwise prescribed by legal authorities.

10.4 Right to Object to the Collection, Use, or Disclosure of Personal Data: The Data Subject has the right to object to the collection, use, or disclosure of their personal data at any time, provided that the data is collected under statutory exemptions from consent, for direct marketing purposes, or for scientific, historical, or statistical research purposes. The Company may decline the request if it can demonstrate compelling legitimate grounds that override the data subject's interests, or if the processing is established for the exercise or defense of legal claims, or statutory compliance.

10.5 Right to Erasure or Destruction: The Data Subject has the right to request the erasure, destruction, or anonymization of their personal data if they believe it has been unlawfully collected, used, or disclosed, or if they deem that The Company no longer requires retention for the purposes specified herein, or upon exercising their right to withdraw consent or object as detailed above.

10.6 Right to Restriction of Processing: The Data Subject has the right to request a temporary restriction on the use of their personal data during periods where The Company is verifying a rectification or objection request, or in any other instance where The Company no longer requires the data but must retain it under relevant laws instead of erasing or destroying it.

10.7 Right to Rectification: The Data Subject has the right to request that their personal data be kept accurate, up-to-date, complete, and not misleading.

11. Penalties

Any responsible person who neglects, omits to order, or fails to perform their duties, or issues orders or takes actions violating this Personal Data Protection Policy and its guidelines, resulting in legal offenses or damages, shall face disciplinary action in accordance with The Company's regulations. The Company shall not compromise on any offenses committed by responsible parties, who shall also bear legal penalties under applicable laws. Furthermore, if such offenses cause detriment to The Company or any third party, The Company reserves the right to pursue further legal action.

12. Policy Review

The Company shall review this policy at least once a year, or in response to statutory amendments.

This Personal Data Protection Policy shall become effective from July 6, 2022, onwards.

-Warapatr Todhanakasem-

(Warapatr Todhanakasem, PH.D.)

Chairman of the Board of Directors

Moshi Moshi Retail Corporation Public Company Limited