(Translation)

-Emblem-	**Re: Personal Data Protection Policy**	Document No.	PTF-PC-022
		Date of Approval:	2024
		Revision No.	00
		Date of Latest Review:	-

Notification No.PTF-PC-022

Personal Data Protection Policy

1. Objectives and Scope of the Personal Data Protection Policy

To comply with the Personal Data Protection Act, B.E. 2562 (2019), and any other relevant laws, including any future amendments to the Personal Data Protection Law, Platinum Fruits Company Limited hereby establishes this Personal Data Protection Policy to outline the details concerning the collection, use, and disclosure of personal data to employees and staff of the Company, or to external personnel and staff of external individuals acting on behalf of or in the name of the Company, in conducting activities related to Personal Data relevant to the Company's business operations, ensuring compliance with the Personal Data Protection Law.

2. Definitions

"Personal data" refers to information about an identifiable individual, whether directly or indirectly, but excluding data of the deceased.

"**Sensitive personal data"** refers to personal data related to race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal record, health data, disabilities, labor union membership, genetic data, biometric data, or any other data that may lead to unfair treatment or impact the individual in a similar manner, as prescribed by the laws protecting personal data.

"Data subject" refers to individuals who own personal data, including customers, business partners, service providers, directors, employees, contacts, and any other individuals from whom the company collects, uses, or discloses personal data.

"Data controller" refers to individuals or legal entities with the authority to decide on the collection, use, or disclosure of personal data.

"Data processor" refers to individuals or legal entities who handle the collection, use, or disclosure of personal data on behalf of the data controller. However, such individuals or entities are not considered data controllers.

"Legal basis" refers to the circumstances under which the law supports the collection of personal data, under the Personal Data Protection Law.

3. Lawful Collection of Personal Data

In collecting, using, or disclosing personal data, the Company shall act in accordance with the legal basis prescribed in the Personal Data Protection Law, as outlined in this policy.

3.1 In the case of general personal data, the collection of personal data shall only be carried out when it meets the conditions of any one of the following legal bases:

3.1.1 Consent from Data Subjects (Consent Basis)

In cases where it is not possible to collect personal data under any other legal basis as specified in sections 3.1.2-3.1.7 of this policy, the Company is required to obtain explicit consent from the Data Subjects before or at the time of collecting Personal Data. Silence or inaction shall not be considered as clear consent from the Data Subjects. Moreover, consent must be in written form or through electronic systems, in formats and texts as prepared by the Company (consent request letter), or as prescribed by law (if applicable). However, if obtaining consent through such means is not feasible, the Data Subject may provide verbal consent, but the Company must record such consent in written form, specifying the details of the consent method and the date of consent.

It is important for the Company to always be aware that consent is deemed valid only when freely and voluntarily given by the Data Subject.

Note: In cases where the Company needs to obtain consent from minors, incapacitated persons, or quasi-incapacitated persons, the Company must obtain consent from the legal representatives with authority to act on behalf of the minors, guardians, or custodians respectively. If the minor is aged 10 years or older, they may provide consent themselves. For instances where the actions are conducted independently by the minors.

3.1.2 For the purpose of creating historical documents or newsletters for public benefit, conducting research, or statistical analysis

The Company may collect personal data for purposes related to the creation of historical documents or newsletters for public benefit, or for research or statistical analysis, provided that appropriate safeguards are implemented to protect the rights and freedoms of the data subjects as prescribed by law.

3.1.3 For the purpose of preventing or mitigating threats to the life, body, or health of individuals (Vital Interests Basis)

In some cases, the Company may find it necessary to collect Personal Data to prevent or mitigate threats to the life, body, or health of any individual, not limited to the Data Subjects. For example, in situations where the Company needs to collect Personal Data due to accidents involving the Data Subjects, the Company is not required to obtain consent for the collection of such Personal Data.

3.1.4 For the purpose of fulfilling contractual obligations between the Company and the Data Subject or for processing requests from the Data Subject prior to entering into a contract with the Company (Contractual Basis)

In cases where the Company needs to collect Personal Data to fulfill a contract with the Data Subject before entering into an agreement with the Company, the Company is not required to obtain consent for the collection of such Personal Data.

3.1.5 For the purpose of performing tasks in the public interest (Public Interest Basis)

In cases where the Company needs to collect personal data to perform tasks for the public interest of the data controller or to exercise state authority delegated to the data controller, the Company is not required to obtain consent for the collection of such Personal Data.

3.1.6 For necessity for the legitimate interests pursued by the data controller (Legitimate Interest Basis)

The Company may collect Personal Data without the consent of the Data Subject in cases where the Company needs to collect data from the Data Subject for the purposes of processing the legitimate interests pursued by the Company or a third party other than the Data Subject. These legitimate interests include but are not limited to the legitimate interests pursued by law in conducting the Company’s business, maintaining security and protecting property

and individuals within the Company's premises, and managing the Company's organization. However, the Company must exercise caution in using this legal basis for the collection of personal data. If it is found that the legitimate interests pursued by law are less significant than the fundamental freedoms of the Data Subject or may significantly impact the fundamental freedoms of the Data Subject, the Company shall not collect Personal Data based on the legal basis of legitimate interests pursued by law, but shall instead obtain consent from the Data Subject if the Company still wishes to collect such Personal Data in the future.

To serve as guidelines for implementing the legitimate interest basis, the Company must assess whether the collection of any Personal Data complies with the following criteria:

A. Whether there is a legal interest benefiting the Company or a third party in collecting the Personal Data.
B. Whether the collection of the Personal Data is necessary for the interests outlined in Item A.
C. Whether the Data Subjects could reasonably expect that the Company may need to collect such Personal Data.
D. Whether the significance of collecting such data is not less than the fundamental freedoms of the Data Subjects or could significantly impact their fundamental freedoms.
E. Whether the Company has implemented appropriate measures to safeguard the collected Personal Data.

3.1.7 <u>To comply with laws applicable to the Company (Legal Obligation Basis)</u>

In cases where the law requires the Company to collect, use, or disclose personal data, the Company is not required to obtain consent from the Data Subjects. This may include actions concerning Personal Data as ordered by a court or government authority. For example, retaining employee data to comply with labor protection laws or keeping accounting documents for the period prescribed by law.

3.2 In the case of sensitive personal data, the Company shall collect, use, or disclose such data only upon obtaining clear consent from the Data Subject, unless there are exceptions as provided by law, including:

- To prevent or mitigate threats to life, body, or health of individuals where obtaining consent from the Data Subject is not possible, regardless of the circumstances. Typically, this includes emergency situations.
- When the data is disclosed publicly with explicit consent from the Data Subject.
- When necessary to comply with the law to achieve the following purposes:
  - Medical, preventive medicine, occupational medicine, or assessment of employee's ability to work.
  - Public health benefits.
  - Labor protection, social security, national health insurance, healthcare benefits according to legal entitlements, where data collection is necessary for the exercise of rights or duties of the Company or the Data Subject.
  - Scientific research, historical or statistical research, or other public interests.
  - Other significant public interests such as collecting sensitive personal data for the purpose of preventing contagious diseases or combating money laundering, and disclosing such data to government agencies for the purpose of preventing and combating money laundering.

Note: The criteria for interpreting the term "public interest" may change according to the guidelines of the Personal Data Protection Committee or as specified in subordinate laws, which may be announced as additional enforcement measures in the future.

3.3 Practices for the Collection of Personal Data

Personal Data shall be collected and gathered only to the extent necessary to achieve the purposes specified by the Company. The Company shall consider and select the Personal Data to be collected as necessary and shall discard or destroy data that may be obtained unnecessarily. Specifically, Sensitive Personal Data shall be treated with utmost caution to mitigate the risk associated with the collection, utilization, and disclosure of personal data without legal authorization by the Company.

In cases where the Company receives more Personal Data than necessary, the Company seeks methods to enable it to retrieve Personal Data only as necessary to achieve the purpose of the collection. For example, in cases where the Company needs to use only Personal Data to identify business partners or their representatives from copies of identification cards, which typically require only general Personal Data for identification purposes, such as name and photograph. Therefore, if there may be sensitive Personal Data appearing on the identification card, such as religion or blood type, the Company should find a way to ensure that such data is not visible on the copy of the identification card when in the possession of the Company. This may involve redacting unnecessary data on the copy of the identification card received, leaving only the data necessary for identification purposes, and so forth.

4. Privacy Notice for Data Subjects

When collecting, using, or disclosing Personal Data, the Company will prepare and provide a Privacy Notice to various types of Data Subjects to explain the details of data processing, definitions, the types of Personal Data to be collected, the purposes of collection, the legal basis for collection, the expected duration of collection, or the expected duration, the types of individuals or entities to which the Personal Data may be disclosed, contact details of the Company, rights of the Data Subjects, and other relevant details. This is to inform, understand, and enable Data Subjects to consider providing consent in cases where the collection of data is not based on a legal basis that allows collection without consent.

The Company must notify or deliver the Privacy Notice to the Data Subject before or at the time of collecting Personal Data unless it is a case where the data has been collected, used, or disclosed before this policy, and the Company also needs to continue collecting, using, or disclosing such data. The Company must promptly notify or deliver the Privacy Notice to the Data Subject.

Notification or delivery of the Privacy Notice may not be necessary if the Company has previously notified or delivered the Privacy Notice to the Data Subject. However, in cases where the company later amends the Privacy Notice, the Company must notify or deliver the amended Privacy Notice to the affected Data Subjects.

5. Source of Personal Data

Generally, the Company must collect Personal Data directly from the Data Subjects. However, if the Company collects Personal Data from sources other than the Data Subjects directly, the Company must promptly inform the Data Subjects of the collection of their Personal Data from other sources and notify them of the Privacy Notice without delay, but no later than 30 days from the date the Company collected the data. The Company must also obtain consent from the Data Subjects for collecting their Personal Data, except when the Company needs to use the data to contact the Data Subjects. In such cases, the Company will notify the Data Subjects upon first contact. Additionally, if the Company intends to disclose the Personal Data, it must inform the Data Subjects before the first disclosure.

However, in some cases, the Company may not be required to notify the Data Subject of the data collection and provide a Privacy Notice if the Company can demonstrate that such notification is impossible or would impede the use or the Company's disclosure of Personal Data or if the Data Subject is already aware of the details. For example, if the Data Subject has previously received a Privacy Notice for certain transactions with the Company and intends to conduct similar transactions with the Company again.

Furthermore, if the Company engages data processors to carry out data processing activities on its behalf, the Company may authorize the data processor to provide the Privacy Notice on behalf of the Company. In such cases, the Company must ensure that the data processor complies with and adheres to this policy, and it shall be deemed that the Company has fulfilled its obligation to notify the details of the data collection, usage, or disclosure as required by the Personal Data Protection Law, as the Company acts as the data controller.

6. Rights of the Data Subject

The Data Subjects have the right to take any action regarding their Personal Data held by the Company, as stipulated by Personal Data Protection Laws. Therefore, the Company must provide a request form for the Data Subject's rights to facilitate the Data Subject's notification of their requests to the Company. However, if the Company needs to refuse the

Data Subject's request for any reason, it must inform the Data Subject of the reasons for such refusal in writing and record the details of the refusal in writing.

6.1 Right to withdraw: The Data Subject has the right to withdraw consent previously given to the Company through a consent letter, whether in whole or in part, and can do so at any time while the Company retains the Personal Data. The company must notify the Data Subject of the consequences of withdrawal, if any, when such withdrawal occurs. However, the consideration of consent shall not affect any actions already taken by the Company based on legally obtained consent from the Data Subject.

Reasons for refusal: Refusal may occur when there are legal limitations on withdrawing consent or when the Personal Data is associated with a contract that benefits the Data Subject.

Response time: Promptly, without undue delay.

6.2 Right to request access to and obtain a copy of Personal Data: The Data Subject has the right to request access to and obtain a copy of Personal Data concerning themselves that is under the responsibility of the Company, or to request disclosure of the source of such Personal Data that they did not consent to.

Reasons for refusal: The Company may refuse such a request only in the following cases:

- When complying with the law or a court order.

- When the Company believes it may adversely affect the rights and fundamental freedoms of others.

In the event of a refusal, the Company must record the refusal along with the reasons in the Company's records.

Response time: If the Company cannot refuse the request, it must respond to the Data Subject's request within 30 days from the date of receipt.

6.3 Right to request to receive and transfer or transmit Personal Data: The Data Subject has the right to request to receive and transfer or transmit Personal Data related to themselves from the Company, or to request the Company to send or transfer data to another person or organization in a generally readable or usable format. This request is applicable only when the Company has collected, used, or disclosed Personal Data with consent, or to fulfill a contract or request made by the Data Subject with the Company.

Reasons for refusal: The Company may refuse such a request if the Personal Data is used for public interest or legal compliance, or if exercising that right would infringe upon the rights and freedoms of others, such as when the data includes trade secrets or intellectual property.

In the event of a refusal, the Company must record the refusal along with the reasons in the Company's records.

Response time: Without undue delay.

6.4 Right to object to the collection, use, or disclosure of their Personal Data : The Data Subject has the right to object to the collection, use, or disclosure of their Personal Data by the company in the following cases:

1. When the collection, use, or disclosure of personal data is for the public interest or legal compliance, including compliance with orders from authorities.

Reasons for refusal: The Company can prove that there is a significant legal basis outweighing the interests, rights, or freedoms of the data subject, or when collecting, using, or disclosing personal data is necessary for establishing, exercising, or defending legal claims.

In the event of refusal, the Company must record the refusal along with the reasons in the Company's records.

2. In direct marketing cases: The Data Subject can object without conditions.

3. For scientific, historical, or statistical research, except when necessary for public interest.

Response time: Without undue delay. If the Company has no grounds for refusal, it must immediately segregate the objected Personal Data from other data as soon as the Data Subject notifies the objection.

6.5 Right to request the deletion, destruction, or transformation of personal data into anonymous data or data that cannot be used to identify an individual, under the following circumstances:

1. The Personal Data is no longer necessary for the purposes for which it was collected, as informed by the Company within the privacy notice.
2. The Data Subject has withdrawn consent, and the company cannot rely on any other legal basis for data processing.
3. The Data Subject has objected to the collection, use, or disclosure of Personal Data, and the Company cannot refuse the objection.
4. The Personal Data was collected, used, or disclosed unlawfully.

   Reasons for refusal: The Company has the right to refuse the request in cases where the Personal Data has been collected, used, or disclosed in the following circumstances:

   - Retaining data for the purpose of exercising freedom of expression, such as in journalistic, academic, artistic, or literary contexts.

- Processing data to achieve historical, statistical, or public interest research purposes or for the compilation of historical documents or records.
- Collecting Sensitive Personal Data when necessary to fulfill legal obligations related to medical care, occupational medicine, employee assessment, or public health benefits.
- Using data for establishing legal rights, compliance, legal claims, or legal defense.
- Processing data to fulfill legal obligations.

If Personal Data has been disclosed to the public by the actions of the Company or transferred to another data controller, and the Data Subject has requested deletion, destruction, or anonymization of such data, the Company must proceed to delete, destroy, or anonymize the data, and must notify the other data controller to take action accordingly.

Response time: Without delay

6.6 Right to request suspension of personal data usage: The Data Subject has the right to request the Company to suspend the usage of Personal Data when:

1. There has been a request for the Company to rectify the accuracy of Personal Data and it is under review. However, the Company may consider lifting the suspension of Personal Data usage if, upon review, it finds that the requested data correction has already been made, notifying the Data Subject prior to lifting the suspension along with the reasons.
2. It is a usage of data not preferred by law, however, the Data Subject requests suspension of usage instead of deletion.
3. The Personal Data is no longer necessary for retention, but the Data Subject has previously requested the Company to retain the data due to necessity for use, establishment, exercise, or defense of legal claims by the Data Subject themselves.
4. The Company is in the process of verifying to refute objections regarding Personal Data. However, the Company may consider lifting the suspension of Personal Data usage if the Company has the right to use the data pursuant to the reasons for objection mentioned above.

   Response Time: Without delay.

6**.7 Right to rectify Personal Data:** The Data Subject may request the Company to take action to ensure that their Personal Data is accurate, up-to-date, complete, and not misleading. However, in the event of refusal of such request by the Data Subject pursuant to the aforementioned right, the Company shall record the refusal along with the reasons in the Company's records for future reference.

Response Time: Without delay.

6.8 Right to lodge a Complaint: The Data Subject has the right to lodge a complaint with the panel of experts appointed by the Data Protection Committee when they perceive that the Company or the data processor, including employees or contractors of the Company or the data processor, has violated or failed to comply with the laws protecting personal data.

7. Duties and Responsibilities of Personnel

All employees and personnel, including contracted individuals and employees of contracted individuals of the Company, have responsibilities to comply with the laws and policies governing this Personal Data Protection, and must maintain confidentiality in handling Personal Data rigorously. They shall not misuse Personal Data obtained during the performance of their duties for inappropriate purposes, for personal gain, or in violation of the law. Duties may be allocated according to hierarchical levels as follows:

7.1 Management Personnel

Have the responsibility to oversee all processes related to Personal Data protection within the Company, as follows:

- Appoint he Data Protection Officer (DPO) or other individuals or units tasked with serving as the central point within the company for overseeing and handling matters related to personal data protection from various departments within the Company shall:
- Assign tasks to employees to establish procedures regarding personal data protection, including practices for managing risks that may arise from the collection, use, or disclosure of Personal Data by the Company, along with guidelines for resolving issues fairly in the event of personal data breaches within the Company.
- Ensure regular control and auditing of compliance with this policy or the appropriateness of this policy.
- Act as the approver for various policy-related operations regarding personal data protection within the Company, or amend or change this policy.
- Consider and approve responses to requests for the exercise of rights by the Data Subject if responding to such requests may significantly impact the company, the Data Subject, and/or any other individuals.

7.2 The Data Protection Officer (DPO) or the person responsible for personal data protection of the Company has the following duties:

has the duty to provide guidance and overseeing all data protection processes of the company.

- Analyze, assess, review, and control all data processing activities of the Company and provide guidance to employees or other units within the Company to ensure compliance with data protection laws.
- Review and approve policies regarding personal data protection within each department of the Company, including methods for managing risks associated with the collection, use, and disclosure of personal data by the Company, and provide guidelines for addressing issues when personal data breaches occur within the Company.
- Analyze, assess, and provide guidance to employees and departments within the Company regarding responses to requests for the rights of data subjects if such responses may significantly impact the Company, data subjects, and/or other individuals.
- Report various incidents related to data processing within the Company to the Chief Executive Officer, Managing Director, and Executives.
- Coordinate and collaborate with the Personal Data Protection Committee Office, including reporting breaches of Personal Data within the specified timeframe.
- Study the Personal Data Protection Act, B.E. 2562 (2019), laws, regulations, or any other related legal matters concerning data protection, as well as monitoring changes or amendments to such data protection laws and informing the Company’s employees.
- Explain, create understanding, and raise awareness among the Company's employees regarding personal data protection and related data protection laws.

7.3 Managerial Level Positions

The responsibilities of managerial level positions involve overseeing the collection, usage, or disclosure of personal data within their respective departments, which may vary according to each department. These duties may be divided as follows:

- Authorizing access to personal data or assigning responsibilities to employees to act as data controllers for managing personal data within various sections of the department.
- Implementing practices and training related to personal data protection within the department and ensuring mutual understanding of which personal data is necessary to collect and which is unnecessary for departmental operations.

- Establishing security measures for personal data within the department to meet legal standards and this policy.
- Approving responses to requests for data subjects' rights and consulting with relevant departments on such matters, including consultations with data protection officers or individuals responsible for the company's data protection, and reporting to management for approval if responding to such requests may significantly impact the company, data subjects, and/or any other individuals.
- Consulting with the service department and the Personal Data Protection Officer to determine appropriate procedures.
- Ensuring records are maintained for the collection, usage, or disclosure of data within the department as specified in this policy.
- Receiving reports from subordinate authorities in cases where breaches of personal data occur and assessing whether such breaches may significantly impact the rights and freedoms of data subjects. This includes consulting with the Personal Data Protection Officer or individuals responsible for the company's data protection and management for appropriate action in accordance with this policy.

7.4 Employee Level Positions

Employees are responsible for strictly adhering to the law and the policies outlined in this Personal Data Protection Policy, particularly in operational aspects, as follows:

- Collecting, using, and disclosing personal data in accordance with the law and this policy, including participation in training related to the company's personal data protection.
- Carrying out assigned duties related to personal data protection operations, such as data management responsibilities concerning security, transmission, disclosure, or recording of data, among others.
- Reporting to superiors in cases where the collection, usage, or disclosure of any personal data within the company, or any orders to do so, are not compliant with the law or may pose risks to the fundamental rights and freedoms of data subjects.
- Notifying superiors for approval in cases where requests to exercise the rights of data subjects are received.

7.5 Contractors and service providers acting as data processors of the Company

Contractors and service providers acting as data processors of the Company shall comply with the laws and policies regarding personal data protection strictly. Additionally, they must be bound by the terms of the Data Processing Agreement entered into with the Company (if any), with responsibilities including but not limited to:

- Collecting, using, and disclosing Personal Data in accordance with the law and this policy, including participation in data protection compliance initiatives of the Company upon request.
- Promptly notify the Company of any Personal Data breaches within 24 hours from becoming aware of such breaches.
- Provide support and assistance to the Company in responding to requests for the exercise of rights by the Data Subject.

Violation of this law and policy by employees may be subject to disciplinary action, and breaches of this law or policy by contractors or service providers acting as data processors of the Company may be considered a breach of contract with the Company as well. If such violations or non-compliance result in damages to the Company, the Company may terminate employment or contracts. Additionally, there may be criminal penalties, including fines and imprisonment, for individuals acting on behalf of the Company who violate or fail to comply with the law. Therefore, employees and relevant parties must familiarize themselves with the laws and policies regarding personal data protection and adhere to them rigorously.

8. Personal Data Protection Measures

The Company shall establish appropriate policy and technical security measures to safeguard the confidentiality, integrity, and availability of Personal Data, aiming to prevent unauthorized access, use, alteration, or disclosure of Personal Data. These measures shall be reviewed when necessary or when technological advancements occur to ensure the effectiveness of security safeguards, in accordance with legal standards.

9. Recording, Usage, and Disclosure of Personal Data

The Company shall ensure that there is documentation of the usage and disclosure of collected data, including but not limited to:

- Personal Data collected, including the purposes and duration of data retention.

- Usage or disclosure of Personal Data in cases of data collection without relying on consent under other legal bases.
- Rights, methods, and conditions for accessing data of the Data Subject.
- Rejection or objection to requests for various types of rights, along with reasons as stated in this policy.
- Description of security measures provided by the Company.

Therefore, to enable the Data Subject to review and enforce their rights as notified or requested to the Company.

10. Transfer of Personal Data to foreign countries or international organizations

The Company may transfer or send Personal Data to foreign countries in the following circumstances:

1. The destination country has been certified to have adequate data protection standards.
2. In cases where the destination country does not have adequate standards, the transfer of Personal Data shall be subject to exceptions under the law, including:
   - Compliance with legal requirements.
   - Obtaining consent from the Data Subject, informing them of the inadequate standards of the destination country or organization.
   - Necessity for the performance of a contract, where the Data Subject is a party to the contract, or for pre-contractual measures requested by the Data Subject.
   - Compliance with agreements between the Company and other individuals or legal entities, for the benefit of the Data Subject.
   - To prevent or mitigate threats to the life, body, or health of the Data Subject or others, when the Data Subject is unable to provide consent at the time.
   - Necessity for the performance of tasks carried out in the public interest.

11. Response to Personal Data breach

In the event of a personal data breach occurring within the Company, where such breach poses a risk to the rights and freedoms of the Data Subject, all employees and staff must collaborate to ensure appropriate legal compliance. The Company shall promptly notify the relevant Data Protection Committee Office of the breach within 72 hours upon becoming aware of the incident, to the extent feasible. In cases where the breach poses a high risk to the rights and freedoms of the Data Subject, the Company shall promptly inform the Data Subject of the breach and provide mitigation measures without delay.

(Translation)

12. Amendment of Personal Data Protection Policy

This Data Protection Policy may be amended or modified as deemed necessary, in accordance with changes in legislation and business appropriateness. The policy shall be reviewed at least once annually.

13. Cookies and Cookie Usage

When you visit our website, the Company may place cookies on your device and automatically collect data. Some cookies are necessary for the website to function properly, while others are used to enhance user experience. Further information regarding cookies can be found in the Company's cookie policy.

14. Additional Information and Reporting Personal Data Breaches

If you have any questions or concerns regarding personal data protection, or if you wish to report a personal data breach, please contact:

- Phone: 0-2171-7821-1
- Email: it@platinumfruits888.com
- No. 59 Romklao 1 Road, Khlong Song Ton Nun Sub-district, Lat Krabang District, Bangkok Metropolis 10520

This Personal Data Protection Policy was approved by resolution of the Board of Directors' Meeting No. 2/2567 dated 28 February 2024. It shall come into effect on 28 February 2024, onwards.