Personal Data Protection Policy

Muang Thai Insurance Public Company Limited

This Policy was approved by the Board of Directors' Meeting No.4/2024 on November 13, 2024.

Contents

Contents

Personal Data Protection Policy

Muang Thai Insurance Public Company Limited

Muang Thai Insurance Public Company Limited has recognized the importance of the protection of personal data of the Company's service users. At present, the information technological advance has greatly influenced the business operations in terms of communication system and work procedures, allowing the collection, use, disclosure and transfer of personal data to foreign countries to be easy, fast and convenient, which may lead to the annoyance or damage in the event of misuse of personal data. As the Office of the Personal Data Protection Commission has prescribed secondary legislation under the Personal Data Protection Act B.E. 2562 (2019), including amended laws for enforcement, it therefore deems appropriate to review this Personal Data Protection Policy to put in place effective personal data protection measures in accordance with the fundamental data protection principles and rights, as well as preventive and remedial measures for the data subjects whose rights to the protection of personal data are violated .

1. Definition

"**Company**" means Muang Thai Insurance Public Company Limited.

"**Service User**" means a person who makes a transaction with the Company or have a business relationship with the Company, for example, a customer, a person who exercises claim under insurance contract, beneficiary, business partner, counterparty, director, attorney, representative, agent, broker, employee, hired staff, person who visits or uses the Company's website, and use an application, device or other channels controlled by the Company, including those whose personal data are collected by the Company such as job applicant and employee and hired staff's families, etc.

"**Personal Data**" means any data relating to a person which enables the person to be identified, directly or indirectly, but does not include the data of deceased person in particular.

"**Sensitive Personal Data**" means personal data as specifically defined in Section 26 of the Personal Data Protect Act B.E. 2562 (2019) and also the version to be amended in the future, such as personal data relating to race, ethnic origin, political opinion, religious or philosophical belief, sexual orientation, criminal record, health data, disability, trade union data, genetic data, biometric data, or any other data which similarly affects the data subject as defined by the Office of the Personal Data Protection Commission.

"**Data Subject**" means a natural person whose personal data enables the identification of such person, and is collected, used and disclosed by the Company.

"**Data Controller**" means a company who makes decision regarding the collection, use or disclosure of personal data of the service user or other person or juristic person that perform the same functions.

"**Data Processor**" means a person or juristic person who operates in relation to the collection, use or disclose the personal data as directed by or on behalf of the Company.

"**Personal Data Protection Committee**" means the committee appointed by the Company which is responsible for overseeing the Company's business operations, as well as considering and making decision regarding the complaint in relation to personal data breach to be in compliance with the policy and practices on the personal data protection.

"**Data Protection Officer**" means a person or a group of persons appointed and designated by the Company in accordance with Section 41 of the Personal Data Protection Act to perform the duties of giving advice, supervising, monitoring of business units, employees, service providers and data processors on behalf of the Company in order to comply with the policies and manuals or guidelines on the personal data protection, including receiving complaints from the service users or data subject, and coordinating with the Office of the Personal Data Protection Commission.

"**Manual or Guideline on the Personal Data Protection**" means a manual or procedure that sets out the methods and conditions of the performance of the business units within the Company, including external service providers, in order to comply with the Personal Data Protection Policy.

"**Person**" means a natural person.

"**Personal Data Protection Laws**" means the Personal Data Protection Act B.E. 2562 (2019) and the version to be amended in the future as well as secondary laws or regulations under the Act, including other applicable laws relating to the personal data protection for the insurance business sector.

"**The Office of the Personal Data Protection Commission or PDPC** " means the government agency, as a juristic person, which is appointed to have the duties and power of supervision and issuance of regulations, measures or practices in relation to personal data protection in accordance with the Personal Data Protection Act B.E. 2562 (2019).

2. Scope of Policy

This Policy applies to the personal data of persons who make transactions or have a business relationship with the Company, both at present and in the future, which are processed by the Company, its employees, hired staff, agents or brokers designated by the Company, including counterparties or third parties who process personal data on behalf of the Company for various products and services via websites, systems, applications and other documents related to the provision of services by the Company, such as insurance application forms, insurance policies, etc., or any other forms of service operated by the Company.

3. Objective

The Company has formulated this Personal Data Protection Policy as a guideline for personal data management for the service users. This includes the collection, use and disclosure of personal data as well as the transfer of personal data to a foreign country in line with the personal data protection laws in order to protect the personal data of the service users. Moreover, the Privacy Notice is established to notify the data subject of the purpose of the collection, use or disclosure of the personal data. In the event that the Company has changed the purpose of any processing related to the personal data, the Company shall notify the data subject for acknowledgement, and request for consent while recording it as additional evidence. This Policy has been considered and approved by senior executives of the Company, placing importance on the protection of personal data of the Company's employees and service users. The Company has announced this Policy to employees and related third parties.

The Company has also developed a manual or guideline on the personal data protection in accordance with this Policy to set out relevant rules and procedures for business units of the Company.

4. Principles of Collection, Use and Disclosure of Personal Data

1. The Company's collection, use and disclosure of personal data of the services users shall be limited to the extent necessary in relation to the lawful purposes and as set forth in this Policy.
2. In collecting, using and disclosing personal data of the service users, the Company shall undertake only with the given consent of the data subject prior to or at the time of personal data collection, along with the notification of privacy notice. The Company shall do so only to the extent necessary according to the purpose of the data subject's consent, except where the collection, use and disclosure of personal data in order to perform duties

or provide services related to insurance contracts, notification of claims, legal duties, or other cases specifically prescribed by personal data protection laws to do so without the consent of the data subject.

3. The collection of personal data from other sources apart from the data subject directly can be carried out only if the personal data protection laws have specifically permitted or exempted.
4. The Company shall not collect, use, and disclose sensitive personal data without the explicit consent of the data subject, except for the collection, use, and disclosure of personal data specifically permitted or exempted from the personal data protection laws.
5. The Company shall ensure that the personal data of the service user remains accurate, up-to-date, complete and not misleading.
6. The Company undertakes to record and/or report on personal data under this Policy and as prescribed by the personal data protection laws, and notify the data processor to record and/or report on record of processing activities in accordance with the rules and procedures prescribed by the personal data protection laws. The Company makes an agreement with the data processor to control the operation of the data processor as stipulated by the personal data protection laws.
7. The Company provides appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, modification or disclosure of personal data, and such measures must be reviewed when it is necessary or as technology changes.
8. The Company prevents other persons or juristic persons from using or disclosing the personal data unlawfully or without authorization.
9. The Company establishes a personal data verification system to erase or destroy the personal data, or anonymize the personal data to become the anonymous data which cannot identify the data subject when the retention period expires, or when it is not relevant or no longer necessary in relation to the purposes for which it was collected, or as requested by the data subject, or where the data subject withdraws consent.
10. The Company is obliged to notify the Office of the Personal Data Protection Commission of the personal data breach within 72 hours after having become aware of it, unless such personal data breach is not unlikely to result in a risk to the rights and freedoms of the persons. In the event that the personal data breach is likely to result in a high risk to the rights and freedoms of the persons, the Company shall notify the data subject of the personal data breach and remedial measures without delay. The notification and

exemption to the notification shall be made in accordance with the rules and procedures prescribed by laws.

11. The Company appoints the Personal Data Protection Committee to perform its functions of considering and reviewing complicated complaints and/or claims with high value of compensation to propose to senior management for consideration, along with supervising business units to comply with this Policy.
12. The Company appoints the Data Protection Officer(s) whose duties are giving advice, supervising, monitoring of business units, employees, service providers, agents, brokers and data processors on behalf of the Company in order to comply with the policies and manuals or guidelines on the personal data protection, including receiving complaints from the service users, data subject or other channels regarding non-compliance with this Policy, and coordinating with the Office of the Personal Data Protection Commission.
13. The data subject shall have the rights to give consent, withdraw consent, access his/her personal data and/or personal data of those whom he/she has the lawful power to act on his/her behalf, object the collection, retention, use and disclosure of his/her personal data and/or personal data of those whom he/she has the lawful power to act on his/her behalf, including the right to rectify his/her personal data and/or personal data of those whom he/she has the lawful power to act on his/her behalf, the right to restrict the retention, use and disclosure of his/her personal data and/or personal data of those whom he/she has the lawful power to act on his/her behalf, the right to erase his/her personal data and/or personal data of those whom he/she has the lawful power to act on his/her behalf, the right to request for the retention, transfer and/or copying of his/her personal data and/or personal data of those whom he/she has the lawful power to act on his/her behalf.

Section 1 : Purposes of Collection, Use and Disclosure of Personal Data

a. The Company shall only collect, use and disclose personal data for lawful purposes and/or for the purposes under this Policy as notified prior to or at the time of such collection.

Unless

1) The new purpose has been notified to the data subject and consent has been obtained before collecting, using or disclosing it;

2) It is necessary for compliance with the law;

3) The data subject has been aware of such new purposes or details, where the personal data protection laws do not require consent to do so;

4) The Company can prove that the notification of such new purposes or details is impossible or will obstruct the use or disclosure of personal data, in particular for achieving the purposes in relation to scientific, historical or statistical researches which the Company has provided appropriate measures to protect the data subject's rights, freedoms and interests;

5) The use or disclosure of personal data shall be carried out on an urgent basis as required by law, and appropriate measures have been implemented to protect the data subject's interests;

6) When the Company is aware of or acquires personal data from his/her duties or occupation or profession and shall maintain the confidentiality of the new purposes as required by law.

b. The Company has a policy to collect personal data directly from the data subject, except for the cases where the Company is required to collect personal data from other sources. The Company shall notify the data subject of the collection of personal data from other sources and details of the collection, use and processing of personal data according to Section 2, without delay within thirty (30) days after the date of collection and the consent of the data subject is obtained, except where the collection of personal data is exempted from obtaining consent or otherwise prescribed by personal data protection laws.

Section 2 : Notification of the Details of Collection, Use and Disclosure of Personal Data or Notification of Privacy Notice for the Data Subject

1. Principles of notification of collection, use and disclosure of personal data

In collecting personal data, unless the data subject is already aware of the details, the Company shall notify the data subject prior to or at the time of collecting personal data of the following details:

1) The purpose of the collection, use and disclosure of personal data;

2) It is for the purpose of compliance with a legal obligation or for the performance of a contract, or where it is necessary to provide personal data for the purpose of entering into a contract, including notification of the possible effect of not receiving such personal data;

3) The personal data to be collected and the period for which the personal data will be retained. In the event that such retention period cannot be clearly specified, the expected data retention period according to the data retention standard shall be specified;

4) The categories of persons or entities to whom the collected personal data may be disclosed or accessed;

5) Information related to the Company, address and contact channels as well as information on the Data Protection Officer, his/her address and contact channels, where applicable;

6) The rights of the data subject as prescribed by personal data protection laws (see Section 4 for details).

Section 3 : Collection, Use and Disclosure of Personal Data

1. Principles for obtaining consent for the collection, use and disclosure of personal data

If the collection, use and disclosure of personal data requires the data subject's consent, the Company shall proceed to obtain consent in accordance with the following rules and conditions:

1) Consent shall be requested prior to or at the time of the collection of personal data;

2) Consent shall be explicitly made in a written statement or via electronic means, unless it cannot be done by its nature;

3) Consent of the data subject for the collection, use and disclosure of personal data shall be requested by taking into account that the data subject's consent is freely given and without unnecessary or irrelevant conditions for entering into such contract and/or provision of services;

4) The purpose of the collection, use or disclosure of personal data shall be notified;

5) The request for consent shall be presented in a manner which is clearly distinguishable from the other matters;

6) The request for consent shall be made in an easily accessible and intelligible form or statement, using plain and clear language, and does not deceptive or misleading to the data subject with respect to such purpose;

7) The request for consent shall be made in accordance with the form or statement as prescribed by the Office of the Personal Data Protection Commission (if any).

In the event that the data subject is a minor

In requesting the data subject's consent, the Company shall proceed as follows:

1) In the event that the minor's giving of consent is not any act which the minor may be entitled to act alone, such act also requires consent of the holder of parental responsibility over the child;

2) Where the minor is below the age of ten (10) years, the consent shall be obtained from the holder of parental responsibility over the child.

In the event that the data subject is incompetent

The consent must be obtained from the custodian who has the power to act on behalf of the incompetent person.

In the event that the data subject is quasi-incompetent

The consent must be obtained from the curator who has the power to act on behalf of the quasi-incompetent person.

2. Exceptions to Requesting for Consent for Collection, Use and Disclosure of Personal Data

The Company can collect, use and disclose personal data without the consent of the data subject for the following purposes:

1) It is for the achievement of the purpose relating to the preparation of historical documents or archives in the public interest, or for the purpose relating to research or statistics, in which the suitable measures to safeguard the data subject's rights and freedoms;

2) It is for preventing or suppressing a danger to a person's life, body or health;

3) It is necessary for the performance of a contract to which the data subject is a party, or in order to proceed at the request of the data subject prior to entering into a contract;

4) It is necessary for the performance of a task carried out in the public interest by the Company, or it is necessary for the exercising of official authority vested in the Company;

5) It is necessary for the legitimate interests of the Company or any other persons or juristic persons other than the Company, except where such interests are overridden by the fundamental rights to the personal data of the data subject;

6) It is necessary for compliance with a law.

3. Exceptions to Requesting for Consent for Collection, Use and Disclosure of Sensitive Personal Data

The Company can collect, use and disclose sensitive personal data without the consent of the data subject for the following purposes:

1) It is to prevent or suppress a danger to life, body or health of the person, where the data subject is incapable of giving consent by whatever reason;

2) It is carried out in the course of legitimate activities with appropriate safeguards by the foundations, associations or non-profit organizations with a political, religious, philosophical or trade union purposes for their members, former members, or persons having regular contact with such foundations, associations or non-profit organizations in connection with their purposes,

without disclosing the personal data outside of such foundations, associations or non-profit organizations;

3) It is information that is disclosed to the public with the explicit consent of the data subject;

4) It is necessary for the establishment, compliance, exercise or defense of legal claims;

5) It is necessary for compliance with a legal obligation to achieve the purposes with respect to;

(a) Preventive medicine or occupational medicine, the assessment of the employee's working capability, medical diagnosis, the provision of health or social care, medical treatment, the management of health or social care systems and services. In the event that it is not for compliance with the legal obligation, and such personal data is under the responsibility of the occupational or profession practitioner or person having the duty to keep such personal data as confidential under the law, it must be for compliance with the contract between the data subject and the medical practitioner;

(b) Public interest in public health, such as protection against cross-border dangerous contagious disease or epidemics which may be contagious or pestilent, or ensuring standards or quality of medicines, medical products or medical devices, on the basis that there is a provision of appropriate and specific measures to protect the rights and freedoms of the data subject, in particular maintaining the confidentiality of personal data in accordance with the duties or professional ethics;

(c) Employment protection, social security, national health security, social health welfare of the entitled person by law, the road accident victim protection, or social protection in which the collection of personal data is necessary for exercising the rights or carrying out the obligations of the Company or the data subject, and the appropriate measures have been provided to protect the fundamental rights and interests of the data subject;

(d) It is for scientific, historical or statistic research purposes or other public interests, which must be carried out only to the extent necessary to achieve such purposes, and appropriate measures have been provided to protect the fundamental rights and interests of the data subject as stipulated by the Office of the Personal Data Protection Commission;

(e) Significant public interest, and appropriate measures have been provided to protect the fundamental rights and interests of the data subject;

Personal data relating to criminal records

In collecting, using and disclosing personal data relating to criminal records, the Company shall do so only under the supervision of a competent legal authority, or the suitable measures have been provided by the Company to protect personal data according to the personal data protection laws. The Company shall collect personal data relating to criminal record for the purposes of recruitment or verification of qualifications, prohibiting characteristics or appropriateness of the persons to be appointed for any position for not longer than six (6) months from the date of the processing of such data for such purpose of each data subject is completed, as prescribed by the Office of the Personal Data Protection Commission, except where otherwise explicit consent is obtained from the data subject.

4. Transferring Personal Data to a Foreign Country

4.1 Transfer of personal data in general cases

In the event that the Company shall send or transfer the personal data to a foreign country, the destination country that receives such personal data shall have adequate data protection standard, and shall be carried out in accordance with the rules for the protection of personal data as prescribed by the Office of the Personal Data Protection Commission.

Except in the following circumstances:

1) It is for compliance with a law;

2) The consent of the data subject has been obtained, provided that the data subject has been informed of the inadequate personal data protection standards of the destination country or international organization;

3) It is necessary for the performance of a contract to which the data subject is a party, or in order to proceed at the request of the data subject prior to entering into a contract;

4) It is for compliance with a contract between the Company and other persons or juristic persons for the interests of the data subject;

5) To prevent or suppress a danger to the life, body or health of the data subject or other persons when the data subject is incapable of giving the consent at such time;

6) It is necessary for carrying out the activities in relation to vital public interest.

In the event that there is a problem with regard to the adequacy of personal data protection standards of the destination country or international organization, such problem shall be submitted to the Office of the Personal Data Protection Commission to decide.

4.2 Transfer of personal data to an affiliated company (if any)

In the event that the Company shall transfer the personal data to an affiliated company located in a foreign country, the Company shall put in place the personal data protection policy regarding the sending or transferring of personal data to another data controller or data processor in a foreign country, and is in the same affiliated company, or in a group, (Binding Corporate Rules: BCRs), and must ensure that such policy has been reviewed and certified by the Office of the Personal Data Protection Commission. The Company shall strictly comply with such reviewed and certified policy, and can carry out the sending or transferring of personal data to a foreign country, and shall be exempted from compliance with the aforementioned rules in general cases.

4.3 Transfer of personal data in the event that adequate personal data protection standards has not been established, and personal data protection policy regarding the sending or transferring of personal data to the affiliated company has not been reviewed and certified

In the event that the adequate personal data protection standards, or the personal data protection regarding the sending or transferring of personal data to the affiliated company have not been put in place, the Company may send or transfer the personal data to a foreign county by providing appropriate protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures in accordance with the rules and methods as prescribed by the Office of the Personal Data Protection Commission.

Section 4 : Rights of the Data Subject

The data subject has the following rights:

1. **Right to withdraw consent for the collection, use and disclosure of personal data**

   The data subject may withdraw his/her consent for the collection, use and disclosure of personal data at any time, **unless** there is a restriction of the withdrawal of consent by law, or a contract which gives benefits to the data subject.

2. **Right to access and obtain data and/or copy of his/her personal data, which is under the responsibility of the Company, or to request the disclosure of the acquisition of the personal data obtained without his/her consent**

   The data subject is entitled to request access to and obtain data and/or copy of his/her personal data, which is under the responsibility of the Company, or to request the disclosure of the acquisition of the personal data which is obtained without his/her consent.

Rejection

The Company can reject the aforementioned request only where it is permitted by law or pursuant to a court order, and such access and obtaining a copy of personal data would adversely affect the rights and freedom of other persons. The record of the rejection together with supporting reasons must be made by the Company.

3. **Right to object the collection, use or disclosure of personal data of the data subject**

The data subject has the right to object the collection, use or disclosure of his/her personal data in the following circumstances:

1) In the event of the personal data collected without consent as follows:

(1) It is necessary to for the performance of a task carried out in the public interest by the Company, or it is necessary for the exercising of official authority vested in the Company;

(2) It is necessary for the legitimate interests of the Company or any other persons or juristic persons other than the Company.

Unless the Company can prove that:

(a) the collection, use, or disclosure of such personal data can be demonstrated that there is a compelling legitimate ground;

(b) the collection, use or disclosure of such personal data is carried out for the establishment, compliance or exercise of legal claims, or defense of legal claims.

2) In the event that the collection, use or disclosure of personal data is for the purpose of direct marketing;

3) In the event that the collection, use or disclosure of personal data is for the purpose of scientific, historical or statistical research, unless it is necessary to performance of a task carried out for the reason of public interest by the Company.

In the event that the data subject exercises his/her right to object, the Company shall no longer be able to collect, use or disclose such personal data, and the Company shall immediately distinguish such personal data clearly from the other matters at the time when the data subject gives the notice of objection to the Company.

In the event that the Company rejects the objection by the reasons in 1) (a) or (b) or 3), the Company shall record such rejection of objection request together with the reasons.

Phongsy

4. **Right to erase or destroy, or anonymize the personal data to become the anonymous data which cannot identify the data subject**

Part 1:

The data subject has the right to request the Company to erase or destroy the personal data, or anonymize the personal data to become the anonymous data which cannot identify the data subject, where the following ground applies:

1) The personal data is no longer necessary in relation to the purpose for which it was collected, used or disclosed;

2) The data subject withdraws consent on which the collection, use, or disclosure of personal data is based on, and where the Company has no legal ground for such collection, use, or disclosure;

3) The data subject objects to the collection, use or disclosure of the personal data as referred in 1) of **3** in **Section 4**, and the Company cannot reject to such request as referred in 1) (2) (a) or (b) of **3** in **Section 4**, or where the data subject exercises the right to object as referred in 2) of **3** in **Section 4**;

4) The personal data has been unlawfully collected, used or disclosed as specified in this section.

Except in the following circumstances:

1) Retention

(1) It is for the purpose of freedom of expression;

(2) It is necessary for compliance with the law.

2) Use

(1) It is for establishment of legal claims;

(2) It is for compliance or exercise of legal claims;

(3) It is for defense of legal claims;

(4) It is necessary for compliance with the law.

Part 2:

Where the Company has made the personal data public, and is requested to erase or destroy the personal data, or anonymize the personal data to become the anonymous data which cannot identify the data subject, the Company shall be responsible for the course of action, both the implementation of technology and the expenses to fulfil the request, and inform other data controllers in order to obtain their responses regarding the action to be taken to fulfil such request.

5. **Right to restrict the use of personal data**

The data subject has the right to request the Company to restrict the use of the personal data in the following cases:

1) When the Company is in the course of examination process in accordance with the data subject's request, to ensure that the personal data is accurate, up-to-date, complete and not misleading;

2) When the personal data which shall be erased or destroyed due to unlawful collection, use or disclosure, but the data subject requests the restriction of the use of such personal data instead;

3) When it is no longer necessary to retain such personal data for the purposes of such collection, but the data subject has necessity to request for further retention for the purposes of establishment, compliance or exercise, or defense of legal claim;

4) When the Company is in the course of verification in order to reject the objection request made by the data subject that the purpose for the collection of the personal data are exempt from obtaining consent.

6. **Right to request the Company to ensure that the personal data remains accurate, up-to-date, complete and not misleading**

The data subject has the right to request the Company to ensure that the personal data is accurate, up-to-date, complete and not misleading.

In the event that the Company does not take action regarding the request of the data subject, the Company shall record such request together with the reasons.

Section 5 : Use of Service Providers

The Company uses the service providers, in accordance with the outsourcing policy, to support the business operations, reduce costs, and enhance the flexibility of operations, including providing the most effective customer services from the experts and specialized service providers.

Principles of the use of service providers in the collection, use, and disclosure of personal data

The Company uses the service providers based on the type or nature of work as well as licensing criteria. The Company shall use the service providers which are well selected in accordance with the selection rules, with responsibility and maximum efficiency for compliance with the contracts and agreements, to prevent the misuse of the service providers which is likely

to result in the conflict of interests and/or corruption.

The Company has provided the explicit and written guidelines for monitoring, evaluation, examination and risk control and management of the use of service providers, in line with the importance and appropriateness of the works, and Risk Management Policy.

The Company shall enter into a data processing agreements with the service providers related to the collection, use and disclosure of personal data in order to control the processing of such data processors in accordance with the criteria and conditions as prescribed by the Personal Data Protection Act and the Company's Personal Data Protection Policy.

Section 6 : Security Measures and Notification of Personal Data Breach

The Company has provided appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of personal data, and such measures must be reviewed when it is necessary, or when the technology has changed in order to efficiently maintain the appropriate security and safety. It shall be in accordance with the minimum standard specified and announced by the Office of the Personal Data Protection Commission. The Company shall also put in place the examination system for erasure or destruction of personal data when the retention period ends, or when the personal data is irrelevant or beyond the purpose necessary for which it has been collected, or when the data subject requests to do so, or when the data subject withdraw consent and notify the Office of the Personal Data Protection Commission of the personal data breach and/or to the data subject, along with the remedial measure without delay.

Section 7 : Contracts and Agreements

The Company has provided the written guidelines or manuals for making contracts and agreements in order to define the scope in relation to the principles of personal data protection, or other laws under this Policy, or other policies of the Company, including other announced rules and regulations, for the effective performance and enforcement of the contracts and agreements for the counterparties. It shall help develop the guideline for drawing up or making the contracts and agreements in accordance with the standard, and ensure that the renewal of contracts and agreements, or the destruction of the expired contracts and agreements are monitored and reviewed.

Section 8 : Training and Communication

The Company has provided training and communication to the employees to enhance knowledge and understanding of the rights, duties and impacts on the operation, which result from the enforcement of the personal data protection laws, this Policy and guidelines on the personal data protection.

Section 9 : Channels for Whistleblowing or Complaints

The Company has put in place the responsible entities for whistleblowing or complaints. The record of the whistleblowing cases or complaints, and the results after receiving them shall be carried out, and such information can be systematically recalled on request or regularly investigated. Such entities have been trained to proceed and communicate with the whistleblower or complainant, and/or those directly involved, both inside and outside the Company, along with enhancing knowledge and understanding of the impacts on the operations under the enforcement of the applicable laws, this Policy and guidelines on the personal data protection.

Section 10 : Business Continuity and Risk Management

The Company has developed a written Business Continuity Plan (BCP), in line with the Company's Risk Management Policy. The allocation of sufficient resources to support the business operations, as well as the assessment, auditing, risk control and risk management have been put in place.

Section 11 : Monitoring, Assessing and Auditing

The Company has provided the explicit and appropriate system for overseeing, monitoring, auditing and assessing the performance under this Policy, in order to ensure the standardized internal control and good service provision, strictly in compliance with relevant regulations. The detailed information on such monitoring, assessing and auditing has been prepared to be accurate for the improvement, development and prompt problem-solving.

Section 12 : Review and Amendment

The Company may review, update, or amend this Policy, as approved by the Company's Chief Executive Officer, without prior notice to the service users. This is to ensure the appropriate and efficient service provision, or compliance with the applicable laws, or regulations prescribed by the regulators, including other notifications or rules announced by the Office of the Personal Data Protection Commission. Unless there is a significant change, the Company shall notify the data

subject of such matter, and/or request the data subject's consent if required by the personal data protection laws.

This Policy shall come into effect from November 13, 2024 onwards.

(Mrs. Nualphan Lamsam)

Chief Executive Officer