Privacy Notice

Your personal information is important to us. That's why we do so much to protect your information, while continually providing Mutual funds, Provident Fund and Private Funds products and services you can count on, regardless of whether or not the account is registered.

This Privacy Notice ("Policy") is meant to help you understand the type of personal information we collect and use, why we use the information, who we may need to share the information with, how we protect your information, as well as data collection period, data destruction and the rights of the Data Subject in order to comply with the Personal Data Protection Act B.E. 2562.

The Policy applies to our website, our mobile applications or online forms, and any other channels that link to this Policy (together, "Platforms"). Depending on the nature of our relationship with you. Please take a few minutes to review this Policy before using our Platforms. **To the extent permissible under applicable law, by using our Platforms you are consenting to the collection, use and disclosure of your information as set forth in this Policy. If you do not agree to be bound by this Policy, you may not access or use our Platforms.**

1. Information collected

Principal Asset Management Company Limited ("Company") collects personal information about you—information that can be used to identify you as an individual. Types of personal information we collect and use when you provide such information through our Platforms include:

1.1 **Identity information** – your name, date of birth, nationality, gender, photograph, identification number (e.g., passport number, tax number, social security number) or other information contained in identity-related documentation (e.g., passport, driver's license, or birth certificate). **We does not wish to collect or use information about race, religion, blood group, or any other information other than the personal information that has been specified above even if such information appears on your ID card, house registration, or any other documents that you voluntarily disclose to us.**

1.2 **Contact information** – e.g., email address, physical address, telephone/fax number;

1.3 **Financial and Transactional information** – your income, assets, liabilities, tax residency, bank details, and other financial information, both current and historical, details about your accounts that you have with us and other details of products and services you have purchased from us, and details about the products and services we provide to you;

1.4 **Technical and Usage information** – details on the devices and technology you use and information about how you use the products and services we provide to you;
1.5 **Communications information** – information we obtain through letters, emails, telephone calls, conversations, social media interactions, or any other correspondence between us;
1.6 **Medical and Health information** – medical and health information required only to provide the products and services you request.

The personal information collected varies depending upon the nature of your relationship with us, how you use the Platforms, and the type of product or service you have with us.

For individuals that login as representatives of a business or corporate account, we may gather information based on your relationship with our organization for the purposes of providing customized services.

For visitors who provide an email address or volunteer other information, such as contact information and/or site registration, we collect this information. Visitors who provide an email address may also be asked to provide feedback about our website via surveys. Additionally, visitors may receive periodic messages from us about new products and services or upcoming events. If you do not want to receive e-mail or other mail from us, please update your subscription and delivery services or click the "unsubscribe" link in the email correspondence received from us.

Mobile applications information

Principal TH and Principal Provident Fund mobile applications allow you to access your accounts using wireless or mobile devices. Our privacy practices apply to any personal information or other information that we may collect through the applications. Additional conditions may apply depending on the specific terms of use and privacy policy of the application. Please refer to the terms of use and other policies for more information about your specific mobile application.

2. The purpose of collecting, using, processing or disclosing your personal information

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

2.1 Where we need to perform the contract, we are about to enter into or have entered into with you;
2.2 Where it is necessary for our legitimate interests (i.e., we have a business or commercial reason for using your information) and your interests and fundamental rights do not override those interests;
- Complying with regulations that apply to us.
- Being efficient about how we fulfill our legal and contractual duties.
- Providing high quality customer service.
- Developing products and services, and what we charge for them.
- Defining types of customers for new products and services.
- Seeking your consent when we need it to contact you.
- Developing and improving the network security, efficiency and technical specification of our IT systems and infrastructure.

- Developing and improving how we deal with and manage financial crime.
- Providing our customers with high quality products, services and Digital Technologies features.
- Keeping our products, services and Digital Technologies features updated and relevant; or

2.3 Where we need to comply with a legal or regulatory obligation; or

2.4 Where you consent. **If you wish to withdraw your consent, you can contact us and can request according to clause 7**

We use your personal information for the following reasons:

- To provide and manage our products, services and Digital Technologies (including any online account with us).
- To create, process and deliver the accounts you hold with us or the products or services you receive from us.
- To comply with our legal and regulatory obligations (including verifying your identity and conducting identity and background checks for anti-money laundering, fraud, credit and security purposes) and to exercise our legal rights.
- To process transactions and carry out obligations arising from any contract entered into between you and us.
- To communicate with you and respond to your inquiries, including responding to complaints and attempting to resolve them.
- To exercise our rights in agreements and contracts to which we are a party.
- To administer auditing, billing and reconciliation activities and other internal and payment-related functions.
- To detect, investigate, report, and seek to prevent financial crime and to manage risk for us and our customers.
- To run our business in an efficient and proper way, including in respect of our financial position, business capability, corporate governance, audit, risk management, compliance, product development, strategic planning, marketing, and communications.
- To send you promotional and marketing materials, newsletters or other related communications (including making suggestions and recommendations to you about services that may be of interest to you).
- To conduct research and analysis to improve the quality of our marketing and the experience of and relationships with our customers.
- To administer and protect our business and our Digital Technologies (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).
- To develop, manage and improve our products, services and the Digital Technologies (including conducting research and analysis) and to test new products, services, and features of the Digital Technologies.
- Medical and Health Information for providing and servicing your policies, accounts, claims or contracts as allowed by the relevant laws protecting your privacy

Failure to provide personal information

Where we need to collect personal information by law or under the terms of a contract we have with you, and you fail to provide that information when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide

you with services). In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

3. Information shared

We may share your personal information to the following categories of recipient:

- **With our business partners.** We may share information with third parties such as companies in the financial business group, our carefully selected business partners, the Stock Exchange of Thailand, Thailand Securities Depository, representatives, custodians, intermediaries and/or other service providers that offer products or services that we believe may be of interest to you in order to achieve your objectives for using our services.
- **With our service providers.** We may disclose information to third party service providers, both onshore and offshore, that perform services for us in the processing or servicing of your account, cloud computing provider, registrar, or with third parties that perform marketing, research, or other services on our behalf. Third parties with whom we may have joint marketing agreements include financial services companies (such as other insurance companies, banks or mutual fund companies).
- **With group companies and affiliates.** We may share the information we collect about you with other member companies of Principal, including Principal International Company, Principal Life Insurance Company, Principal Global Investors and their affiliates for a variety of purposes. For example, we share information to assist us in providing service and account maintenance, to help us design and improve products and to offer products and services that may be of interest to you.
- **With offshore securities companies and asset management companies.** We may disclose Beneficial Owner information to offshore securities/asset management companies by referring to compliance with foreign laws.
- **With third parties as permitted or required by law.** This includes disclosing your information to regulators, law enforcement authorities, tax authorities and credit bureaus. This information is only disclosed as required or permitted by law, and in accordance with established company procedures. We may transfer and disclose the information we collect about you to comply with a legal obligation, including responding to a subpoena or court order, to prevent fraud, to comply with an inquiry by a government agency or other regulator, to address security or technical issues, to respond to an emergency, or as necessary for other lega lpurposes.
- **As part of business transitions.** In relation to an ongoing or proposed business transaction your information may be transferred to a successor organization. If such a transfer occurs, the successor organization's use of your information will still be subject to this Policy and the privacy preferences you have expressed to us.
- **Other** –
    - Agents and advisers who we use to help run your accounts and services, collect what you owe, and explore new ways of doing business;
    - Fraud prevention agencies;
    - Any party linked with you or your business's product or service;
    - Companies we have a joint venture or agreement with;
    - Organizations that introduce you to us;
    - Companies that we introduce you to;
    - Companies you ask us to share your data with.

In addition, we may share non-personal (anonymized) information, such as aggregate data and Usage Information with other third parties.

Except as described above, or as set forth in a separate privacy policy, we will not provide your personal information to other third parties without your specific consent.

4. Automatic data processing

Under your explicit consent, we may use your personal data for automated processing, which may affect your personal information or for other data collection. If you wish to withdraw consent, you can contact us and can request according to clause 9.

5. Rights of the Data Subject

Under certain circumstances, you have rights under PDPA in relation to your personal information:

- **Right to withdraw consent at any time**: This applies where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
- **Request access to your personal data**: This enables you to request a copy of the personal data we hold about you and to check that it is accurate and that we are processing it lawfully. This is not, however, an absolute right, and the interests of other individuals may restrict your right of access. For additional copies requested, we may charge a reasonable fee based on administrative costs.
- **Request correction of your personal data**: This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request transfer of your personal data:** This enables you to request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Request erasure of your personal data:** This enables you to ask us to delete or remove personal data where there is no lawful basis for us continuing to process it. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Request restriction of processing:** This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

- **Object to processing of your personal data:** This enables you to object to processing of your personal data where we are relying on a legitimate interest and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. We will provide you with appropriate choices to opt-in or optout as set out above in our Policy.
- **Make a complaint:** You have the right to make a complaint at any time to the relevant data protection supervisory authority. We would, however, appreciate the chance to deal with your concerns before you approach your supervisory authority.

We require that your request be in writing. In addition, we may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response. We try to respond to all legitimate requests within a reasonable period and not exceeding the time specified by law.

In the event that you request us to delete, destroy, limit the data processing, suspend, transform your personal information into a form that does not personally identify the owner of the personal information or withdraw your consent, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

6. How we protect your information

We understand the importance of appropriately safeguarding information you provide to us. It is our practice to protect the confidentiality of this information, limit access to this information to those with
a business need, and not disclose this information unless required or permitted by law.

We have security practices and procedures in place to protect data entrusted to us. These procedures and related standards include limiting access to data and regularly testing and auditing our security practices and technologies.

All employees are required to complete privacy, security, ethics and compliance training. We also offer a wide variety of other training to all employees and temporary workers to help us achieve our goal of protecting your information.

Ultimately, no website, mobile application, database or system is completely secure or "hacker proof." While no one can guarantee that your personal information will not be disclosed, misused or lost by accident or by the unauthorized acts of others, we continuously review and make enhancements to how we protect customer information.

Data Transfers

The data that we collect from you may be transferred to, and stored at, a destination outside Thailand. We share your personal data within the Principal Financial Group which will involve transferring your data outside Thailand. Furthermore, many of our external third parties are based outside Thailand so their processing of your personal data will involve a transfer of data outside Thailand.

Where we transfer personal data to a destination outside Thailand, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented: (a) We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data; and (b) Where we use certain service providers, we may use specific contracts which give personal data the same protection it has in Thailand.

7. Retention of data

In the event that you terminate your business relationship with us, we will keep your personal information for a period of 10 years. It may not always be possible to completely remove or delete all of your information from our databases without some residual data because of backups and other reasons. We will retain your information for as long as your information is necessary for the purposes for which it was collected. For example, we may retain your personal data if it is reasonably necessary to comply with any legal obligations, meet any regulatory requirements, resolve any disputes or litigation, or as otherwise needed to enforce this Policy and prevent fraud and abuse. If requested by a law enforcement authority, we may also retain your personal data for a period of time. To determine the appropriate retention period for the information we collect from you, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of the data, the purposes for which we process the data, whether we can achieve those purposes through other means, and the applicable legal requirements.

8. Changes to this Policy

We are continually improving and adding to the features and functionality of the services we offer through our Platforms. As a result of these changes (or changes in the law), we may need to update or revise this Policy. Accordingly, we reserve the right to update or modify this Policy at any time, without prior notice, or providing any notice required under applicable law.

You may access the current version of this Policy at any time on the company website www.principal.th.

9. Contact us

If you have any questions about this Policy, or about how we collect and use your personal information
or if you would like to exercise any rights you may have in relation to your personal information, please
contact us at:

- Principal Asset Management Co., Ltd. no. 44 CIMB Thai Bank Building 16th Fl, Langsuan Road, Lumpini, Pathumwan, Bangkok, Thailand 10330
- **Call Center (662) 686 9500**
- Data Protection Officer) email: DPO@principal.th
- company website www.principal.th.