

Announcement No. 11/2020

HR Privacy Policy

SBI Thai Online Securities Co., Ltd. ("we", "our" or "us"), the employing company, is committed to protecting the privacy and security of our current, former, and retired employees, and non-employed workers ("you" or "your") and your Personal Data. The purpose of this HR Privacy Policy (the "Policy"), is to give you information about how we collect, use, disclose, and/or cross-border transfer your Personal Data (as defined below), and your rights in relation to your Personal Data in connection with your employment.

We need to collect, use, disclose, and/or cross-border transfer your Personal Data in order to enter into our contract of employment with you and to continue to perform crucial aspects of your contract of employment, such as paying you and providing you with benefits. If we are not able to carry out the activities with respect to collection, use, disclosure, and/or cross-border transfer of your Personal Data described in this Policy, we may not be able to comply with your contract of employment, and in some instances, we may not be able to accept your employment or continue your employment.

This Policy is not part of your employment contract, and we may update this Policy from time to time. We will notify you the most recent version of this Policy or obtain your consent again if there are material changes to this Policy, or if we are required to do so by law. It is recommended that you periodically revisit <K:\HR Department\pdpa> for the latest version of this Policy.

1. Personal Data we collect about you

"Personal Data" means any identified or identifiable information about you as listed below. As part of your employment with us, we might collect your information in a variety of ways. For instance, we may request Personal Data directly from you or indirectly from various sources (e.g. your supervisor, public authorities, outsourced HR providers, social media, online platforms, and other publicly available sources).

We will collect, use, disclose and/or cross-border transfer the following categories and types of Personal Data about you, including but not limited to:

- identification data and contact details, such as your full name, date of birth, nationality, address, email, phone number, ID card, and passport;
- other personal information, such as your marital status, data of children, emergency contact details and beneficiaries;
- job-related information, such as your position, title, department, contract details, resume, recruitment history, and application form;
- information about your salary and benefits, such as payroll information, salary, remuneration, and entitlement to benefits and other applicable benefits;
- bank account information;
- information on absences, such as the dates of leaves of absence or vacation and other leave taken by you;
- disciplinary information, such as employee misconduct or misbehavior;
- evaluation records, such as your performance assessments and performance reviews;
- academic background, such as education history, completed transcript, education certificate;
- military status; and
- securities holding information and other related information.

"Sensitive Data" means Personal Data classified by law as sensitive data. We will only collect, use, disclose, and/or cross-border transfer Sensitive Data if we have received your explicit consent or as permitted by law.

We will collect, use, disclose and/or cross-border transfer the following Sensitive Data about you:

- biometric data (such as finger scan);
- health data (such as drug test results, medical information, and annual health check-up record);
- criminal records; and
- race and religion.

If you provide the Personal Data of any third party (such as your spouse, beneficiary, emergency contact, referral, references, and other persons related to your securities holding) to us, e.g. their name, family name, telephone number, and relationship with you, you represent that you have the authority to do so and to permit us to use the Personal Data in accordance with this Policy. You are also responsible for notifying the third party of this Policy and/or obtaining consent from the relevant third party, if required.

2. Purposes and legal bases

Your Personal Data and Sensitive Data are collected, used, disclosed, and/or cross-border transferred by us to carry out a variety of activities that are related to your employment and our compliance with obligations as your employer and as a business, for the purposes as follows.

2.1 The purposes for which your consent would be required for Sensitive Data

We rely on your consent to collect, use, disclose and/or cross-border transfer your Sensitive Data for the following purposes:

- biometric data, such as finger scanning for building access;
- criminal record and health data, to consider an application for hiring decisions, background screening, and monitoring;
- race and religion data, for the purpose of equal opportunities and diversity; and
- statistical and analytical purposes, for the improvement of our work force and employment practices.

Where legal basis is consent, you have the right to withdraw your consent at any time. This can be done so, by contacting Human Resources Department, contact number 02-022-1400. The withdrawal of consent will not affect the lawfulness of the collection, use, disclosure, and cross-border transfer of your Sensitive Data based on your consent before it was withdrawn.

2.2 Purposes for which we may rely on other legal grounds in collecting, using, disclosing, and cross-border transferring your Personal Data

We rely on the following legal grounds to collect, use, disclose, and/or cross-border transfer your Personal Data: (a) a contractual basis, for our initiation or fulfillment of employment contract with you; (b) a legal obligation; (c) the legitimate interest of ourselves and third parties, to be balanced with your own interest and fundamental rights and freedoms in relation to the protection of your Personal Data; (d) vital interest, for preventing or suppressing a danger to a person's life, body, or health; and (e) public interest, for the performance of a task carried out in the public interest or for the exercise of official actions.

If you are a job applicant, we rely on the legal grounds in (a) to (e) above for the following purposes of collection, use, disclosure, and/or cross-border transfer of your Personal Data:

- to process your application for an internship, part-time job, temporary job, or employment;
- for individual verification and contact purposes;
- for applicant evaluation and scoring so as to make a hiring decision;
- for suitability evaluation;
- for salary or compensation payment and the offer of reimbursements;

- for background screening if you are offered a position with us;
- to communicate with your designated contacts in case of an emergency; and
- for other purposes as reasonably required by us as set out in the job application or any relevant documents.

If you are our employee or non-employed worker, we rely on the legal grounds in (a) to (e) above for the following purposes of collection, use, disclosure, and/or cross-border transfer of your Personal Data:

- for recruitment purposes, such as making hiring decisions or changing the type of employment contract (e.g. changing your position from an intern, temporary worker or part-time job to a regular employee);
- to provide necessary training, tools, and equipment and on-boarding processes;
- for salary, compensation and provision of benefits, such as payroll, bonuses, and welfare;
- for internal organization management, such as resource allocation, internal audits, and administration;
- for leave administration in compliance with our work rules;
- for communication purposes, including the provision of references and recommendations;
- for statistical and analytical purposes so as to improve of our work force and employment practices;
- for compliance with legal obligations, such as labor, health, and safety requirements, or as requested by governmental agencies;
- to maintain employee disciplinary records for effective management or to impose disciplinary action when necessary;
- to conduct internal investigations to follow up on complaints or claims, monitor employee misbehavior, and prevent fraud;
- to communicate with designated contacts in case of an emergency;
- to prevent illegal employee activities or the omission of duties;
- to protect our information secrecy and assets; and
- for other purposes as reasonably required by us in connection with your employment (such as to proceed with the activities or operation for us or on behalf of us) or as set out in your employment agreement, the work rules, or any documents related to HR.

Failure to provide certain information when requested, to the extent permitted by law, may affect our performance of contractual or legal obligations, which may affect your recruitment process, employment, or work engagement determination, or withdrawal of an employment offer.

3. To whom we may disclose or cross-border transfer your Personal Data

We may disclose or transfer your Personal Data to the following third parties who process Personal Data in accordance with the purpose under this Policy. These third parties may be located in or outside Thailand. You can visit their privacy policies to learn more details on how they process your Personal Data.

- **Group of company:** Your Personal Data may be accessible to or shared with other entities within our group for data analytic, company performance reporting, risk management or auditing purpose within our group.
- **Government agencies:** We share your Personal Data with different governmental authorities and agencies, as required by law for the purposes of regulatory compliance or legal obligation (e.g. the court, Office of the Securities and Exchange Commission, Stock Exchange of Thailand, Bank of Thailand, Revenue Department, foreign tax authority, Ministry of Labour, Social Security Office, Department of Skill Development, Legal Execution Department, Student Loan Fund, and National Office for Empowerment of Persons with Disabilities).

- **Other third parties:** We may also transfer or allow access to your Personal Data to third parties, such as our business partners and service providers (e.g. provident fund managers, banks, payment processors, insurance companies, hospitals, visa or work permit agencies, HR consultant companies, HR information system service providers, training service providers, or financial service providers) to process your Personal Data for the aforementioned purposes as set out in Section 2 of this Policy.

When we transfer Personal Data to the third parties, we will take steps to ensure the protection of your Personal Data, such as confidentiality arrangements, appropriate security measures to the extent as required by law.

4. Cross-border transfer

We may disclose or transfer your Personal Data to third parties or servers located overseas, and the destination countries may or may not have the same data protection standards as Thailand. We will take steps and measures to ensure that your Personal Data is securely transferred, that the receiving parties have suitable data protection standards in place, and that the transfer is lawful by relying on the derogations as permitted under the law.

5. How we retain your Personal Data

We retain your Personal Data for as long as is reasonably necessary to fulfill the purposes for which we have obtained them as set out in this Policy and to comply with our legal and regulatory obligations. However, we may have to retain your Personal Data for a longer duration, if required by any applicable law.

6. Minor's Personal Data

Our activities (including recruitment process, employment activities and activities with non-employed workers) are generally not aimed at minors and we do not knowingly collect Personal Data of minors, quasi-incompetent persons and incompetent persons. If you are minor, quasi-incompetent or incompetent person wishing to engage employment or contractual relationship with us, you must obtain consent of your parent or guardian prior to contacting us or providing us with your Personal Data. If you are a minor who is above the age of ten years but has not reach the legal age (20 years of age or by marriage), you are required to obtain consent from the holder of parental responsibility over you.

7. Your rights in relation to your Personal Data

Subject to applicable laws and exceptions thereof, you may have the following rights:

- **Access:** you may have the right to access or request a copy of the Personal Data we are processing about you;
- **Data Portability:** you may have the right to obtain Personal Data we hold about you, in a structured, electronic format, and to transmit this data to another data controller;
- **Objection:** in some circumstances, you may have the right to object to how we process your Personal Data in certain activities;
- **Deletion:** you may have the right to request that we delete or de-identify your Personal Data that we process about you, e.g. if the data is no longer necessary for the purposes of processing;
- **Restriction:** you may have the right to restrict our processing of your Personal Data if you believe such data to be inaccurate, that our processing is unlawful, or that we no longer need to process this data for a particular purpose;
- **Rectification:** you may have the right to have Personal Data that is incomplete, inaccurate, misleading, or out-of-date rectified;

- **Consent withdrawal:** you may have the right to withdraw consent that was given to us for the processing of your Personal Data, unless there are restrictions on the right to withdraw consent as required by the law, or there is a contract that gives benefits to you; and
- **Lodge a complaint:** you may have the right to lodge a complaint to the competent authority if you believe our processing of your Personal Data is unlawful or non-compliance with applicable data protection law.

8. Contact details

If you wish to contact us to exercise your rights relating to your Personal Data or submit a complaint or any questions in relation to the collection, use, and disclosure of your Personal Data under this Policy, please contact:

SBI Thai Online Securities Co., Ltd.

- 1768 Thai Summit Tower, 31st Floor, New Petchburi Road, Bangkapi Sub-district, Huaykwang District, Bangkok 10310
- www.sbito.co.th/pdpa

Data Protection Officer

- Head of Compliance and Internal Audit Department.
- 1768 Thai Summit Tower, 31st Floor, New Petchburi Road, Bangkapi Sub-district, Huaykwang District, Bangkok 10310
- E-Mail: SBITO_compliance@sbito.co.th
- Phone number 0-2022-1454, 0-2022-1484

By the resolution of the Board of Directors' Meeting No.2/2020 held on May 22, 2020.

The Policy shall be effective from May 25, 2020.

KO
x 小川 和也

(Mr. Kazunari Ogawa)

Chief Executive Officer & Authorized Director

