(Unofficial Translation)

Announcement of the Office of the Board of Investment

on Personal Data Protection Policy and Practice Guidelines

of the Office of the Board of Investment, B.E 2565 (2022)

To protect personal data in official contacts with the Office of the Board of Investment and to comply with the Personal Data Protection Act, B.E. 2562 (2018) and international standards in the collection, storage, use, disclosure, or any management of personal data that require transparency and accountability;

By virtue of Section 6 and Section 7 of the Royal Decree Governing Criteria and Methods in Conducting Electronic Transactions for the Government Sector, B.E. 2549 (2006) and Section 37 of the Personal Data Protection Act, B.E. 2562, the Office of the Board of Investment issues the following announcement:

1. The Announcement of the Office of the Board of Investment on Policy and Practice Guidelines for Personal Data Protection of the Office of the Board of Investment, B.E 2561 (2018), dated July 11, 2018, shall be revoked, and substituted with the following announcement:

2. This announcement is called the "Announcement of the Office of the Board of Investment on Personal Data Protection Policy and Practice Guidelines of the Office of the Board of Investment, B.E 2565 (2022)"

3. Scope of application.

This announcement applies to a data subject who is a natural person, or a natural person representing a juristic person, who contacts the Office of the Board of Investment and whose personal data is processed by the Office, officials, employees, contracting parties, or third parties processing the data on behalf of or in the name of the Office.

The data subjects include:

(1) Officers or operators, employees

(2) Business partners and service providers who are natural persons

(3) Board members, authorized representatives, agents, and shareholders

(4) Users of services provided by the Office

(5) Visitors or users of the websites, applications, devices, or other communication channels

(6) Other individuals whose personal data is collected by the Office, such as the family members of the officers or job applicants, etc.

4. Definitions.

"Office" means the Office of the Board of Investment.

"personal data" means any information about a natural person that enables the identification of such a person, whether directly or indirectly, but excluding data about a deceased person.

"sensitive personal data" means information about race, ethnicity, political opinions, cults, religious or philosophical beliefs, sexual orientation, criminal records, health, disabilities, labor unions, genetic data, biometric data, etc.

"data processing" means any operation performed on personal data, such as collection, recording, copying, organizing, storing, updating, altering, using, recovering, disclosing, disseminating, publicizing, transferring, combining, deleting, destructing, etc.

"data subject" means a natural person who owns the personal data that the Office collects, uses, or discloses.

"data controller" means the Office, a natural or juristic person that has the authority and responsibility to decide on the collection, use, or disclosure of personal data.

"data processor" means the Office or a natural or juristic person that processes personal data on the instructions or behalf of the data controller. This natural or juristic person, while involved in the processing, does not act as the personal data controller themselves.

5. Collection, classification, and use of personal data

The Office collects or obtains various types of personal data from the following sources:

(1) Direct collection from data subjects through multiple service channels such as application processes, approval, permission, registration, job applications, signing of contracts or documents, filling out surveys, using products or services, or any other service channels operated by the Office. This includes cases when data subjects contact the Office at the headquarters or through other contact channels under the Office administration.

(2) Collection from data subjects when they use websites for products or other services under contracts or obligations, by using cookies or software on the data subjects' devices to monitor their use behavior on the Office's website or the Office's product and services.

(3) Collection from sources other than the data subjects. The Office may collect personal data from sources other than the data subjects, provided that these sources have lawful authorization or consent from the data subjects to disclose the information to the Office. This includes acquiring data via digital service

integration by government agencies for broader public benefits to the data subjects. Personal data collection from other state agencies is part of the Office's mission to establish a central data exchange center to support government agencies' operations in providing services to the public via digital technologies. The service delivery requirement specified in agreements may entail the exchange of personal data with counterpart contracting agencies. If data subjects refuse to disclose information required for the Office's service operation, the Office may be able to offer services to the data subjects only partially or not at all.

6. Legal basis for personal data collection

The Office considers and specifies the legal basis for the collection of personal data under the Personal Data Protection Act, B.E. 2562 (2019) as follows:

Legal Basis for Personal Data Collection	**Description**
The Performance of duties in accordance with the laws	To enable the Office to fulfill its mission of promoting investment in accordance with the Investment Promotion Act, B.E. 2520 (1977), the National Competitiveness Enhancement for Targeted Industries Act, B.E. 2560 (2017), the Computer Crimes Act (No. 2), B.E. 2560 (A.D. 2017), the Official Information Act, B.E. 2540 (1997), and other laws on public administration, including actions in compliance with court orders and other laws.
The performance of contractual obligation	To fulfill its duties according to the contractual obligations or to take the necessary actions to enter into a contract in which the data subject is a contracting party with the Office. This covers contracts of employment, outsourcing, a memorandum of understanding for collaboration, and other agreements.
Consent from Data Subjects	In cases where the Office must obtain consent from the data subjects to collect, use, and disclose personal data, the purposes for data collection, use, and disclosure must be clearly outlined and communicated to the data subjects before seeking the data subject consent. For instance, the collection of sensitive personal information for purposes that do not fall under the exceptions specified in Sections 24 or 26 of the Personal Data Protection Act B.E. 2562, or the presentation and promotion of products and services of a contractual partner or business affiliate, and so on.

Legal Basis for Personal Data Collection	Description
The purpose of achieving the public interest or the use of state authority entrusted to the Office.	To enable the Office to utilize state authority and accomplish its mission for the public interest in accordance with the duties specified by laws, regulations, directives, and cabinet resolutions
Necessity for Legitimate Interests	For the legitimate interests of the Office and other individuals, where such interests hold significance no less than the fundamental rights regarding personal data of the data subjects. This includes, for instance, utilizing data for maintaining security of the Office's building and premises, or processing personal data for internal administrative purposes of the Office.
Necessity for Preventing or Suppressing Dangers to Life, Body, or Health.	To prevent or suppress dangers to a person's life, body, or health, such as through providing application services for epidemic surveillance in compliance with Government policies.
For historical Documentation, Research, or Significant Statistics.	To enable the Office to create or support the preparation of historical documents, research, or statistics.

7. Types of personal data collected by the Office.

Types of Personal Data	Description and Examples
Personally, Identifiable Information	Information that identifies a person or data in official documents indicating specific personal information, such as title, first name, last name, middle name, nickname, signature, national ID number, nationality, driver's license number, passport number, household registration data, professional license number (for each profession), social security number, health insurance number, etc.
Personal Characteristics Data	Detailed data such as date, month, and year of birth, gender, height, weight, age, marital status, military conscription status, photographs, spoken languages, behavioral information, preferences, bankruptcy status, information on being incapacitated or quasi-incapacitated, etc.

Types of Personal Data	Description and Examples
Contact Data	Contact data such as home telephone number, mobile telephone number, fax number, email address, home postal address, social media usernames (e.g., Line ID, MS Teams), and residence locations. etc.
Work and Education Data	Employment details, including work and educational records, such as types of employment, profession, rank, position, duties, expertise, work permit status, reference person information, taxpayer identification number, position assumption records, employment records, salary information, starting and ending dates of employment, performance evaluations, welfare and benefits, assets in possession of the personnel, work achievements, bank account numbers, educational institutions, educational qualifications, academic results, and graduation dates.
Data Related to the Use of the Office's Services	Data related to the use of Office's products or services, such as user account names, passwords, PINs, Single Sign-On (SSO ID) information, OTP codes, computer traffic data, location data, photographs, videos, audio recordings, usage behavior data (websites under the Office's supervision such as www.boi.go.th or various applications), search history, cookies or similar technologies, device ID, types of devices, connection details, browser information, working languages, and operating systems.
Sensitive Personal Data	Sensitive personal data, such as; race, religion, disability information, political opinions, criminal records, biometric data (facial recognition data), and health information.

8. Purposes of personal data collection

(1) For utilization in accordance with the duties, authorities, regulations, and laws that fall under the responsibility of the Office.

(2) To use in operating transactions of the Office.

(3) To supervise, use, monitor, audit, administer, and manage service provision to facilitate and meet the data subjects.

(4) To maintain and update personal data and reference documents of data subjects.

(5) To prepare records of personal data processing in compliance with applicable laws.

(6) To analyze data and resolve problems related to the Office's services.

(7) To undertake necessary internal organizational management, including personnel recruitment, selection of board members or other positions, and qualification evaluation.

(8) To prevent, detect, avoid, and investigate frauds, security breaches, or prohibited or illegal activities that may cause damage to the Office and the data subjects.

(9) To confirm and verify identities and check information when the data subjects register for the Office's services, contact the office for services, or exercise legal rights.

(10) To enhance and modernize the quality of products and services offered by the Office.

(11) For risk assessment and management.

(12) To notify, confirm orders, communicate, and update information to the data subjects.

(13) To prepare and deliver necessary and relevant documents or data.

(14) To confirm identity, prevent spam, or unauthorized or illegal actions.

(15) To monitor both individual and collective usage of the Office's services by data subjects for research and analysis purposes.

(16) To undertake necessary actions to comply with the Office's duties and responsibilities towards the supervisory agencies, tax authorities, law enforcement, or any legal obligations of the Office.

(17) To conduct necessary operations for the legitimate interests of the Office or other individuals or juristic persons related to the Office's activities.

(18) To prevent or suppress danger to an individual's life, body, or health, including epidemic disease surveillance and control.

(19) To prepare historical documents for public benefit, research, or statistical compilation as the Office has been assigned.

(20) To comply with laws, decrees, enforceable orders, or legal proceedings, including handling data in compliance with court orders and exercising the data-related rights of data subjects.

9. Cookies

The office collects and utilizes cookies, along with similar technologies, on websites under the Office's supervision, such as www.boi.go.th, or on devices or services used by the data subjects. This is to maintain security for the Office's service operation and to facilitate users' convenience and a positive

experience. The data will be used to improve the Office's website in alignment with the data subject's preferences. Users can manage or delete cookie usage on their own through settings in their web browser.

10. Use of personal data

Types of Data Recipients	Details
The Office may disclose information for legal compliance or other significant purposes (such as for the public benefit).	Law enforcement agencies or authorities with supervisory or regulatory control, or other important objectives, such as the Cabinet, the Acting Minister, the Department of Business Development, the Revenue Department, courts, the Office of the Attorney General, the Department of Disease Control, the Ministry of Digital Economy and Society, etc.
Committees related to the Office's legal operations.	The Office may disclose the personal data of the data subjects to individuals holding positions in various committees, such as the Board of Investment and the Investment Promotion Sub-committee.
Contracting parties providing welfare services to the Office's personnel.	External parties contracted by the Office to provide welfare services, such as hospitals, banks, telephone service providers, etc.
Business partners	The Office may disclose the data subject's information to partners working with the Office for the purpose of providing services to the data subject. This includes service agencies contacted through the Office's services, marketing service providers, advertising media, financial institutions, platform service providers, telecommunications service providers.
Service Providers	The Office may delegate or assign other entities to provide services on its behalf or support its operations. This includes data storage services such as cloud computing, system development, software and application development, website services, document delivery services, payment processing services, internet service providers, telephone services, digital ID services, social media services, risk management services, external consulting, and transportation services, ~~among others~~ etc.

Types of Data Recipients	Details
Other Types of Data Recipients	The Office may disclose information to other types of data recipients, such as the Office's contacts, hospitals, educational institutions, and other agencies. The purposes of the disclosure are, for example, for the Office's service operations, training activities, award receptions, charity events, or donations.
Public Disclosure	The Office may disclose data publicly, when necessary, such as when the Office is mandated to announce information in the Royal Gazette or to comply with Cabinet resolutions.

11. Duration of personal data retention and disposal

The Office will retain personal data only for a period that is necessary according to the collecting purposes, as defined in policies, announcements, or relevant regulations. At the end of the period when the data becomes unnecessary for the specified purposes, the Office will delete, destroy, or anonymize the data to render the data subject unidentifiable. These processes will adhere to the formats and standards to be specified by the Office's PDPA committee, or to international standards. However, ~~in the cases of disputes, the exercise of rights, or legal proceedings related to the personal data of the data subject,~~ the Office reserves the right to maintain the data in the cases of disputes, the exercise of rights, or legal proceedings related to the personal data of the data subject until the matter is resolved or a final court judgment is issued."

12. Service provision by a third party or a service subcontractor

The Office may assign or hire a third party (personal data processor) to process personal data on behalf of or in the name of the Office. This third party may offer services in various capacities, such as hosting, service subcontracting, cloud computing servicing, or other forms of commissioned work.

In outsourcing personal data processing to a third party as a data processor, the Office will establish an agreement defining roles and responsibilities of both the Office, as the data controller, and the third party, as the data processor. This agreement will specify in detail the types of personal data ~~in detail~~ that the Office may assign for processing, as well as the processing purposes, scope, and other pertinent terms. The third-party processor shall process the data within the scope of the agreement and as directed by the Office only and not process the data for any other purposes.

In cases where the data processor outsources data processing tasks to a subcontractor (sub-processor) on behalf of or in the name of the data processor, the Office will oversee to ensure an agreement is

made between the data processor and the sub-processor. The agreement's standards and format shall not be lower than those of the primary agreement between the Office and the data processor.

13. Protection of personal data security.

The Office will implement data protection measures by restricting access to personal data exclusively to specific personnel or authorized individuals who need to use the data for the purposes notified to the data subjects. These persons shall strictly follow the Office's data protection protocols and maintain the confidentiality of personal data encountered during their duties. The Office has established both organizational and technical security measures in alignment with international standards and the directives announced by the Personal Data Protection Committee.

Additionally, when the Office transmits, transfers, or discloses personal data to third parties, for reasons such as fulfilling its mission, contractual obligations, or other agreements, the Office will implement suitable and lawful measures to safeguard data security and confidentiality to ensure the ongoing safety and protection of the collected personal data.

14. Data subject participation rights

(1) Right to access personal data: Data subjects are entitled to access their personal data held by the Office, receive copies, and inquire about sources of the data. However, the Office reserves the right to reject the request due to lawful justifications, ordered by a court, or if granting access adversely impacts the rights and freedoms of others.

(2) Right to correct personal data: Data subjects are entitled to request modifications to their personal data to bring it up to date, or ensure its accuracy, completeness. If the data are found inaccurate, incomplete, or obsolete, the data subject may request amendments to maintain the data's precision, relevance, and completeness, and to avoid misinterpretations.

(3) Right to erase or destroy personal data: Data subjects have the right to request the Office to delete, destroy, or anonymize the data, making it unable to identify the data subjects. The right for deleting or destroying personal data is subject to conditions prescribed by applicable laws.

(4) Right to request suspension of data use: Data subjects are entitled to request the Office to suspend the use of their personal data under the following circumstances:

(a) When the Office is in the process of verifying the data for completeness and ~~currency~~ recency, as per the request of the data subject for data amendment.

(b) The personal data of the data subject has been collected, used, or disclosed unlawfully.

(c) When the personal data is no longer necessary for collection purposes, as informed to the data subject, but the data subject requests the Office to continue retaining their personal data to support their legal right exercise.

(d) While the Office is assessing the lawfulness of collecting, using, or disclosing the personal data of the data subject, or examining the necessity of the collection, use, and disclosure of the personal data in the public interest. This applies when the data subject has exercised their right to object to the collection, use, and disclosure of their personal data.

(5) Right to object to personal data processing: Data subjects have the right to oppose the collection, use, or disclosure of the personal data unless the Office has lawful reasons to reject the request. (For example, the Office can demonstrate that the collection, use, and disclosure of the personal data has been executed on superior lawful justifications, or for establishing legal claims, complying with legal responsibilities, exercising legal rights, or acting in the public interest.)

(6) Right to withdraw consent: If a data subject has provided consent to the Office for the collection, use, or disclosure of personal data, the data subject has the right to withdraw the consent at any time while the Office maintains the data. However, right to withdraw consent is subject to exceptions in the case that the Office is legally mandated to retain the data or any contractual agreements that mutually benefit the data subject and the Office are still in effect.

(7) Right to receive, send, or transfer personal data: Data subjects are entitled to request their personal data from the Office in a format that is generally readable on automated equipment or devices and can be used or disclosed through automated means. They also have the right to request the Office to transfer such data to other data controllers. The use of this right must adhere to conditions specified in the relevant laws.

15. The Personal Data Protection Law imposes criminal, administrative, and civil penalties for non-compliance or violation of the provisions. Therefore, officials and related individuals must strictly adhere to these laws, as well as the Office's policies, and practice guidelines.

16. Revision of the personal data protection policy.

The Office may periodically update, amend, or revise its policy and practice guidelines to enhance efficiency and effectiveness. These changes will be communicated to data subjects via the website, www.boi.go.th. Utilizing the Office's products or services following the implementation of the policy update shall be deemed acceptance of the amended policy and guidelines.

The Information and Communication Technology Center will review and update the policy and practice standards at least once a year or in case of any significant changes in the Office.

17. Contacting the Office of the Board of Investment

Data subjects who have any inquiries, suggestions, or concerns regarding the collection, usage, and disclosure of personal data by the Office or, regarding this policy, or who wish to exercise their rights under the personal data protection laws, may contact:

(1) Data Controller

Contact Address: The Office of the Board of Investment.

555 Vibhavadi-Rangsit Road, Chatuchak Bangkok.

Email: datacontroller@boi.go.th Tel: 02-553-8111

(2) Data Protection Officer (DPO)

Contact Address: The Office of the Board of Investment.

555 Vibhavadi-Rangsit Road, Chatuchak Bangkok.

Email: datacontroller@boi.go.th Tel: 02-553-8111

18. All agencies under the authority of the Office of the Board of Investment and authorized persons by the Office have the duty to protect personal data in accordance with the laws and standards specified as follows:

(1) Information Security Management System (ISMS) Manual.

(2) Information and Communication Technology (ICT) Security Policy.

(3) Statement of Applicability (SOA)

(4) Information Risk Assessment Approach

(5) Risk Assessment Report

(6) Risk Treatment Plan

(7) Business Continuity Plan (BCP)

(8) The Operations Manual and Procedures for Information Security Management System according to the ISO/IEC 27001 Standard of the Office of the Board of Investment.~~nt.~~

19. This announcement is effective from the date following the announcement date onward.

Announced on February 14, 2022

(Ms. Duangjai Asawachintachit)

Secretary General of the Board of Investment