

### **Purpose and Scope of Personal Data Protection Policy**

To comply with the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws, including any future amendments (**the "Personal Data Protection Law"**), Irene Enterprise Co., Ltd. (the "Company") has created this Personal Data Protection Policy ("**Policy**") to explain in detail of the collection, use, and disclosure of personal data to the Company's employees and staff, or to the individuals outside the Company who act on behalf of the Company or in name of the Company in processing related to personal data that relevant to the Company's business operations that shall be conducted to the Personal Data Protection Law.

### **Key Definitions**

**"Personal Information"** means information relating to an natural person which enables that person to be identified, whether directly or indirectly, but does not include information about the deceased person in particular.

**"Sensitive Personal Data"** means personal data relating to race, ethnicity, political opinions, creed beliefs, religion or philosophy; Sexual behavior, criminal record, Health Information, Disability, Labor union data, genetic data, biometric data, or any other data that may cause unfair discrimination against the personal data subject or affect the individual similarly, as prescribed by the Personal Data Protection Law.

**"Personal Data Subject"** means a natural person who is the owner of personal data, i.e., customers, business partners, service providers, directors, staffs, employees, visitors, and any other natural persons whose personal data is collected, used, or disclosed by the Company.

**"Personal Data Controller"** means the company which has the authority to make decisions regarding the collection, use, or disclosure of personal data.

**"Personal Data Processor"** means a natural person or juristic person who collects, uses, or discloses personal data according to the order or on behalf of the personal data controller, however the Personal Data Processor, whether natural or juristic person, is not be the Personal Data Controller.

**"Legal Bases"** means the lawful grounds to collect and process the Personal Data as prescribed in the Personal Data Protection Laws.

### **Collection of Personal Information**

To collect, use, or disclose the Personal Data, The Company shall act under the legal bases stipulated in the Personal Data Protection Law, which the Company has set forth as follows:

#### **1. General Personal Information**

- Title, name-surname (in any language), national Identification number, date of birth, age, gender, status, address, photograph, map drawing or location of address, signature, phone number, ID Line

- Academic level, field of study, educational institution, grades or GPA, start and graduation years, work experience, job title, employment period, salary, benefits, competency fees, position fees, and training documentation.
- Passport information, visa information, notification of stay over 90 days of the foreigner, work permit information, and official government documents issued for foreigner (copy format)
- Copy of house registration, copy of driver's license, copy of educational qualification, copy of the front page of bank account passbook, copy of name change certificate, copy of secondary certificates such as salary certificate, employment certificate, training certificate, etc.
- Personal details of vehicles, such as car band, vehicle type, registration number
- Personal Data of Third Parties. I consent to allow Irene Enterprise Co., Ltd. collecting personal data of third parties that I provide to the Company (e.g. references, emergency contacts, guarantors, assignees, and/or beneficiaries).
- Information related to electronic systems usage, such as e-mail, IP address, browser type (web browser), and cookies. (Cookies) chat history in various applications.

The Company will collect personal data in accordance with the conditions

either of the following legal bases:

#### **1.1 Consent from the Data Subject (Consent Base)**

In cases the data cannot be collected with other legal bases as specified in clause 1.2. – 1.7 The Company is required to obtain explicit consent from the Personal Data Subject before or at the time of collecting Personal Data through hand-writing or electronically systems which may contain formats and messages prepared by the Company (Letter of Consent) or as prescribed by law (if applicable). If obtaining consent through these methods is not feasible, the Data Subject may provide verbal consent. The Company shall record this verbal consent, specifying the details of the consent method and the date on which the consent was given. The Data Subject has the right to withdraw consent at any time unless there is a legal or contractual restriction that limits the Data Subject's rights.

The Company will request consent from the Personal Data Subject when the Personal Data Subject provides consent freely and voluntarily.

**Note:** If the Company seeks consent from minors who have not reached legal age, incapacitated individuals, or quasi-incapacitated individuals, the Company must obtain consent from the legal guardian with authority over such minors, legal guardians, or caretakers, respectively. In the case of minors aged 10 years or older, they may provide consent independently. However, consent must be granted for the benefit of the minor."

**1.2 For the preparation of historical documents or archives for the public interest. Research or Statistics (Archival Base/Research/Statistics)**

If the Company is required to collect personal data to prepare historical documents or archives for the public interest, or related to research or statistics, with appropriate protection measures in place to protect the rights and freedoms of the personal data subject, as required by law.

**1.3 To prevent or suppress danger to life or a person's health (important benefits to life)**

If the Company is required to collect personal data to prevent or suppress danger to the life, body, or health of any individuals and not limited solely to the Data subject, for example, when the Company is obliged to collect personal data due to an emergency accident that occurs to the personal data subject. In this case, the Company does not require consent to collect personal data.

**1.4 To perform the contract between the Company and the Data Subject or to take steps at the request of the Data Subject before entering into a contract with the Company (Contract Base).**

If the Company is obliged to collect personal data to perform a contract to which the personal data subject is a direct party to the Company or to act at the request of the personal data subject before entering into a contract with the Company. The Company does not require consent to collect such Personal Data.

**1.5 To perform duties in carrying out tasks for the public interest (public interest base).**

If the Company is required to collect personal data to perform its duties in carrying out its tasks for the public interest, the Company or perform duties in exercising the authority vested in the Company. The Company does not require consent to collect such Personal Data.

**1.6 For legitimate interests (based on legitimate interests)**

If the Company is required to collect personal information without seeking consent from the Personal Data Subject for the purpose of carrying out activities related to the legitimate interests pursued by the Company or a third party, the Company is not required to seek consent to collect such personal data. This includes legitimate interests pursued by the Company or a third party for the Company's business operations, security and protection of assets and individuals within the Company's premises, organizational management of the Company, etc. However, the Company must exercise caution in using this legal basis for data collection and must ensure that the legitimate interests pursued under this basis do not outweigh the fundamental freedoms of the data subjects or significantly impact their fundamental freedoms. If it is determined that the legitimate interests pursued do not outweigh the data subject's fundamental freedoms, or if there is a significant impact on the data subject's fundamental freedoms, the Company must obtain consent from the data subject before continuing to collect their personal data. To apply this legal basis, the Company must evaluate whether the data collection complies with the following criteria for each case."

To guide the application of legitimate interest bases. The Company shall evaluate whether the collection of any Personal Data complies with the following criteria in all respects:

(1) Whether the Company or a third party has a legitimate interest. In collecting such personal information.

(2) Whether the collection of personal data is necessary for the interests under clause (1).

(3) Whether the Data Subject should have anticipation that the Company may need to collect such Personal Data.

(4) Whether the collection of such data is no less important than the fundamental rights and freedoms of the personal data subject, or is it not the case that it may significantly affect the fundamental rights and freedoms of the personal data subject.

(5) Whether the Company have appropriate personal data protection measures in the collection of such personal data.

#### **1.7 To comply with laws applicable to the Company (legal basis)**

If the Company is required to collect Use or disclose personal data to comply with the law. The Company is not required to obtain consent from the Data Subject. This may include processing personal data following court orders or government officials. For example, the retention of personal data of employees for compliance with labor protection laws. Retention of accounting documents for the period specified by law, etc.

**2. Sensitive Personal Data** Nationality, religion, criminal record, health information, disability data, biological data (e.g., fingerprint simulation data; facial and iris image simulation data), the Company collects Sensitive Personal Data may be used, used or disclosed **only with the explicit consent** of the Data Subject (details in Clause 1.1), Unless exempted by law, as follows:

- It is the prevention or suppression of danger to life. or the health of the person to whom the personal data subject is unable to give consent. For any reason (emergency use)
- It is information that is disclosed to the public with the explicit consent of the personal data subject.
- It is necessary to comply with the law to achieve objectives regarding:
  - Medical and occupational medicine services, employee capacity assessment
  - Public Health Benefits
  - Labor protection, social security, national health insurance, benefits related to medical care rights of legally entitled individuals, and any necessary actions based on the duties or responsibilities of the Company or the data subject
  - Scientific, historical, or statistical research or other public interest.

- Other important public interests, such as collecting sensitive personal data for the purpose of preventing infectious diseases or epidemics, or collecting, using, and disclosing such data to state agencies for the purpose of preventing and suppressing money laundering

Note: The guidelines for consideration and interpretation of the term "public interest" may be subjected to change according to the guidelines for the consideration and definition of the Personal Data Protection Committee or as specified in subordinate laws which may be enacted in the future.

### 3. Personal Data Collection Practices

Personal data will be collected only as necessary to achieve the purposes defined by the Company. The Company will consider and choose to collect data as necessary and discard or destroy information that may be obtained unnecessarily, especially sensitive personal data, to reduce the risk of unlawful collection, use, and disclosure of personal data by the Company.

If the Company receives more personal data than necessary. The Company shall find ways to enable the Company to retain Personal Data to the extent necessary to achieve the purpose for which it was collected, such as in the case where the Company uses Personal Data to identify business partners or representatives of the Company's partners from copies of ID cards, the Company typically needs only general personal data for identification purposes (e.g., name and photograph). In such case, If sensitive personal data may appear on the ID card (e.g., religion, blood type), the Company will use the method to prevent such information from appearing on the copy of the card when it is in the possession of the Company, which may cross out unnecessary information in the copy of the ID card that he or she has obtained, leaving only the information necessary for identification, etc.

### 4. Respect for Rights and Protection of Personal Data

The Company respects the rights of personal data of data subjects and realizes that data subjects wish to obtain security regarding their data. Personal data collected and collected by the Company will be utilized only for the relevant purposes and notified. The Company has measures to maintain security as well as prevent the unlawful use of personal data as **Technical Measures and Organizational Measures** to prevent personal data breaches, losses, etc. access, destruction, use, modification, modification, use or disclosure of information outside the purpose or without authority;

### 5. Purposes of Collection, Use, and Disclosure of Personal Data

The Company collects, uses, and discloses Your personal data for the following purposes:

#### Business Objectives

- For the benefit of product provision and distribution including providing or receiving various forms of service
- For financial and tax transaction related with the Company's contractual obligations

- For research and analysis purposes
- For the benefits of creation of database for analyzing and presenting any services or products of the Company and its affiliates or persons who are vendors, agents, or related to the Company.
- For the benefit of improving the quality of operations. Provision of services and operations related to the Company's business

#### Corporate Objectives

- For job application with Irene Enterprise Co., Ltd.
- For human resource management operations, employee profile records, issuance employee cards, parking permits, training and development applications, and related activities
- For identity verification purposes with financial institutions related to credit transactions of the data subject.
- For the benefit of applying for various benefits both internally and externally.
- For communication and coordination in work-related activities of affiliated units and other departments.
- Purposes under Section 24 of the Personal Data Protection Act B.E. 2562 (2019)
  - To achieve objectives related to the preparation of historical documents, research studies, or statistics, for which appropriate safeguards have been put in place.
  - To prevent or suppress the danger to life. physical or personal health.
  - It is necessary for the performance of a contract to which the personal data subject is a party, or to take steps at the request of the personal data controller before entering into such contract.
  - It is necessary for the performance of a task carried out in the public interest or the exercise of state authority vested in the personal data controller.
  - It is necessary for legitimate interests.
  - It is the legal duty of the personal data controller.
- For the purpose of access control, prevention, and suppression of danger to life. or the health of you or others. Control and prevention of communicable diseases and for the benefit of maintaining the safety of buildings, buildings, and areas of the Company.
- To comply with current and future laws or regulations applicable to the Company, the Personal Data collected by the Company for the above purposes is necessary for the performance of contracts or compliance with applicable laws. If you do not provide such necessary personal data, it may violate

the law, or the Company may not be able to administer or manage contracts or facilitate various operations for you.

#### **6. Personal Data Storage and Retention Period**

The Company employs both physical documents and/or electronic data storage methods. Physical documents are stored in restricted-access locations and/or on servers and/or cloud services provided by third-party vendors. Personal data will be retained for a duration necessary to fulfill the purposes of collection, use, and disclosure of the data, as specified in the criteria for data retention

The retention period will be determined by the Company based on its ongoing relationship with you as a stakeholder and may be extended if required to comply with other applicable laws. This extension is within the limits set by this law, primarily for the purpose of legal claims, law enforcement, exercising legal rights, initiating legal actions, or for other reasons in accordance with the internal policies and regulations of the Company

#### **7. Security measures for the retention of personal data**

The Company acknowledges the critical importance of maintaining the security of personal data. The Company implements appropriate measures to ensure the security of personal data and to align with the principle of maintaining data confidentiality. These measures include encryption methods, access controls, and restrictions on unauthorized modification, access, or disclosure of data. Additionally, access to personal data is limited to authorized personnel, excluding employees, contractors, and representatives without relevant affiliations to prevent data loss, unauthorized access, alteration, usage, or disclosure, without proper legal authority or consent.

#### **8. Data Breach Case Management**

The Company places significant importance on maintaining personal and information security, including data leakage management. If it is found that the security of the Company's personal information collection has been compromised or the personal information that the Company has stored has been disclosed to relevant third parties as a result of the Company's activities, it is not limited to Information security attacks. The Company will make reasonable efforts to notify individuals who may be affected by the data breach and who might face consequences arising from the exposed personal data. This includes notifying affected parties about the risks involved and any potential mitigation steps that may reduce the impact of the data breach. These actions will be in compliance with the Personal Data Protection Act, B.E. 2562(2019).

#### **9. Disclosure of Personal Data to Other Persons or Entities**

The Company may need to disclose personal data to group companies or other persons or entities that are strategic partners both domestically and internationally. who work with the Company to provide products and services in various ways, or as reasonably necessary to enforce the Company's terms and conditions or in the event of a

reorganization; Personal information may be disclosed to government agencies or government agencies following legal regulations or court orders or orders of competent authorities. Personal information will be kept confidential, both in hard copy and electronic format.

#### **10. Cookies Policy**

"Cookies" means small computer files that store necessary temporary personal data on the data subject's computer. These are necessary for facilitating efficient and convenient communication during interactions with the website. When accessing the website [www.irene-enterprise.com](http://www.irene-enterprise.com), data related to website access will be stored in the form of cookies. This Cookie Policy explains the meaning of their function, their purposes, as well as instructions for deleting or rejecting cookies for privacy. By accessing this website, the data subject is considered to have granted permission for the Company to use cookies in accordance with this Cookie Policy

#### **Privacy Notice for Personal Data Subjects**

The Company will engage in the collection, use, or disclosure of personal data. The company will prepare and notify the **Privacy Notice** to various types of personal data subjects to clarify the details of data processing. Definitions Personal Data to be collected, the purpose of collection, legal basis for the collection, period of collection or anticipated period, category of persons or entities to whom Personal Data may be disclosed to that person or entity, detailed contact information about the company, the Data Subject and other concerned information to know, understand, and consider giving consent if the collection is not within the legal basis that can be collected without consent.

The Company shall notify or deliver the **Privacy Notice** to the Personal Data Subject before or while collecting Personal Data unless it is the case of collecting Personal Data that the Company has collected. The Company is still required to collect, use or disclose such information. The Company shall notify or deliver the Privacy Notice to the Data Subject as soon as possible.

Notification or delivery of the **Privacy Notice** may not need to be repeated if the Company has previously notified or delivered the Privacy Notice to the Data Subject. The Company shall notify or deliver the revised Privacy Notice to the new personal data subject.

#### **Sources of Personal Data**

The Company has a policy to collect personal data directly from the personal data subject. If the Company collects personal data from other sources, the Company will notify the collection of personal data and privacy notice to the personal data subject without delay but not later than 30 days from the date the Company collects and the Company will also seek consent from the personal Data Subject. In the case of collecting personal data based on consent, except in cases where the Company is required to use such personal data to contact the personal data subject,

the Company will notify the Data Subject upon the first contact. The Company will notify the Data Subject before the first disclosure of the Personal Data. In some cases, the Company may not be required to notify such collection information and privacy notice to the Personal Data Subject. If the Company can prove that such notification is not possible or will hinder the use or disclosure of the Company's Personal Data, or the Data Subject is already aware of such details, such as the Data Subject has already received a privacy notice for certain transactions with the Company and wishes to do the same transaction with the Company again.

If the Company has hired a personal data processor to act on behalf of the Company. The Company may require the Personal Data Processor to provide the Privacy Notice on behalf of the Company, which the Company will supervise the Personal Data Processor to comply with this Policy and treat it as if the Company had informed the Company of details about the collection, use, and personal data processing, use or disclosure personal data following the duties prescribed by the Personal Data Protection Law as the Company is the data controller.

#### **Rights of the Data Subject**

The Company shall be aware that the Data Subject has the right to take any action against his/her Personal Data which is in the possession of the Company as stipulated in the Personal Data Protection Law. To facilitate the Data Subject in requesting to exercise various rights with the Company. however, If the Company has reason to refuse to exercise the rights of the Data Subject, the Company shall notify the Data Subject of the reasons for such refusal in writing and record the reason for such refusal in writing.

**1. Right to withdraw consent** The Data Subject has the right to withdraw the consent which has been given to the Company through the consent letter. Whether to withdraw part or all consent and can be done throughout the period that the Company retains personal data. The Company will also notify the data subject of the impact upon withdrawal. The withdrawal of consent will not affect any actions that the Company has previously done due to obtaining lawful consent from the personal data subject.

**Grounds for refusal:** In case of restriction of the right to withdraw consent by law or in case of personal data related to a contract that benefits the personal data subject.

**Response time:** without delay

**2. Right to access and obtain a copy of personal data** The Data Subject has the right to request access to and obtain a copy of the Personal Data concerning themselves which is under the Company's responsibility, or to request the disclosure of the acquisition of such Personal Data without his/her consent.

**Grounds for refusal:** The Company may reject a request to enforce this right only in the following cases:

- to comply with a law or court order, or
- When the Company deems that it will affect the fundamental rights and freedoms of other persons.

However, if the Company fails to Request the Data Subject following the above rights The Company will record the rejection of the request together with the reasons in the Company's transaction record.

**Response Time:** In case the company cannot refuse. The Company will process the request of the personal data subject within 30 days. From the date of receipt of the request

**3. Right to request receipt and transfer of personal data** The Data Subject has the right to obtain Personal Data concerning themselves from the Company or request the Company to send or transfer the Data to other persons or organizations in a format that is readable or generally usable, including the right to obtain his/her Personal Data collected by the Company or other persons or organizations that have been transferred. This request is only applicable if the Company has collected, used, or disclosed personal data with consent or to perform a contract or request before entering into a contract between the personal data subject and the Company.

**Grounds for refusal:** The company may reject a request if the personal data in question is used for public interest or legal obligations, or if granting such a request would infringe on the rights and freedoms of others, such as when the personal data contains trade secrets or intellectual property information

**.Response time:** without delay

**4. Right to object to collection, use, or disclosure of personal data** The Personal Data Subject has the right to object to the collection, use, or disclosure of the Company's Personal Data in the following cases:

(1) It is the collection, use, or disclosure of personal data for legitimate or public interests, including compliance with orders of government officials.

**Grounds for refusal ( for item 4 (1)):** The Company can prove that there are legitimate grounds that are more important than the interests, rights, or freedoms of the Personal Data Subject, or that the Personal Data is collected, used, or disclosed for the establishment, establishment, use or disclosure of Personal Data. comply with, exercise, or defend legal claims;

However, if there are grounds for rejecting the request of the personal data subject according to the above rights. The Company will record the rejection of the request together with the reasons in the Company's transaction record.

(2) Direct Marketing Case, the personal data subject can object unconditionally.

(3) For scientific, historical, and statistical research, unless it is necessary for the public interest.

**Response Time:** Without delay and if the Company has no grounds for rejection. The Company will immediately separate the above Personal Data from other data from the date the Data Subject notifies the objection.

**5. Right to request erasure** The Personal Data Subject has the right to request the Company to delete, destroy or anonymize the Personal Data, or make it non-reusable when:

(1) The personal data is no longer necessary to be retained for the purpose for which it was collected, within a timeframe that may be stated in the privacy notice

(2) The personal data subject has withdrawn consent and the Company cannot use other legal bases for collecting data.

(3) The personal data subject has objected to the collection, use, or disclosure of Personal Data and the Company cannot reject the objection.

(4) Personal data has been unlawfully collected, used, or disclosed.

**Grounds for refusal:** The Company has the right to reject the request. In the following cases:

- It is preservation for exercising freedom of expression.
- To achieve objectives on a basis relating to the preparation of historical documents or archives, research, statistics, or public interest bases.
- It is the collection of sensitive personal data which is necessary for the performance of legal obligations for preventive medicine, occupational medicine, evaluated employee ability, and Public Health Benefits
- Use for the Establishment of Legal Claims Complying with or exercising legal claims or defending legal claims
- Use for the performance of legal obligations

If the personal data has been disclosed to the public by the Company's actions or transferred to another data controller and the personal data subject has requested to delete, destroy or anonymize such data. The Company must comply with the request to delete, destroy or anonymize such Personal Data and must notify other Data Controllers to comply with the request.

**Response time:** without delay

**6. Right to restrict the use of personal data** The Data Subject has the right to request the Company to suspend the use of Personal Data. On:

(1) The personal subject has requested the company to correct their personal data, and the company is in the process of verification. However, the company may consider lifting the suspension if it verifies that the requested correction has been made to the accurate data. The personal data owner must be informed before lifting the suspension along with the reasons.

(2) It is an unlawful use of data, but the data subject requests to suspend the use instead of deleting it.

(3) Personal data is no longer necessary to be retained, but the data subject has previously asked the Company to retain the data because it is necessary for use. The Establishment complies with or raises against the legal claims of the personal data subject.

(4) The Company is in the process of proving to reject the objection to the personal data. However, the Company may consider lifting the suspension of the use of Personal Data if the Company deems that the Company has the right to continue using the Data on the grounds of denying the right to object to the aforementioned Personal Data.

**Response time:** without delay

**7. Right to rectification** The Data Subject may request the Company to rectify their Personal Data to be accurate, up-to-date, complete, and not misunderstanding.

However, if there are grounds for rejecting the request of the personal data subject according to the above rights. The Company will record the rejection of the request together with the reasons in the Company's transaction record.

**Response time:** without delay

**8. Right to complain:** The Data Subject has the right to complain to the Personal Data Protection Committee. When it is deemed that the Company or the Personal Data Processor, including its employees or contractors or the Data Processor, violates or fails to comply with the Personal Data Protection Law.

### **Duties and responsibilities of personnel**

All employees and personnel, including hired persons and employees of persons employed by the Company, are obliged to comply with the laws and this Personal Data Protection Policy and shall strictly maintain the confidentiality of personal data and shall not misuse personal information received during the performance of work duties. Use for personal gain or unlawful use with the hierarchical division of duties as follows:

#### **1. Managing Director and Management Personnel**

Responsibilities: Overseeing all personal data protection procedures of the Company as follows:

- Designate an individual or units acting as a Data Protection Officer (DPO) and/or other persons or agencies to be the center of the Company in taking care of and receiving matters related to personal data protection from various departments within the Company.
- Assign tasks to employees to determine personal data protection practices, including practices to manage risks that may arise from collection, collection, and personal data collection. Use and disclose

personal data by the Company along with guidelines to solve concrete problems when personal data breaches occur within the Company.

- Provide regular control and check compliance with this policy or the appropriateness of this policy.
- Approve the implementation of various policies related to personal data protection, such as arranging for a review of the appropriateness of this policy or the protection of personal data within the company or amending this policy.
- Consider and approve in responding to requests to exercise the rights of the personal data subject if responding to such requests may have a significant impact on the Company, Personal Data Subject and/or any other person

## **2. Data Protection Officer (DPO) or person responsible for personal data protection of the Company**

Responsibilities: Providing advice and inspecting all personal data protection procedures of the Company as follows:

- Analyze, assess, inspect, and control the Company's personal data processing activities and provide advice to personnel or other departments within the Company to ensure that the Company's personal data processing activities comply with the Personal Data Protection Law and the Company's Personal Data Protection Policy.
- Review and approve the guidelines on personal data protection of each unit within the Company, including practices for managing risks that may arise from the collection, use, and use of personal data protection. Use and disclose personal data by the Company and guidelines for solving problems when personal data breaches occur within the Company.
- Analyze, evaluate, and advise personnel and departments within the Company regarding responses to requests to exercise the rights of the personal data subject if responding to such requests may have a significant impact on the Company. Data Subject and/or any other person
- Report incidents related to the processing of personal data within the Company to the Managing Director and executive personnel.
- Coordinate and cooperate with the Office of the Personal Data Protection Committee, including reporting personal data breaches that occur within the Company to the Office of the Personal Data Protection Committee within the period stipulated by law.
- Study the details of the Personal Data Protection Act B.E. 2562 (2019), rules, announcements, orders, regulations, or any other laws related to personal data protection, including monitoring changes or amendments to such personal data protection laws and informing the Company's personnel.

- Explain, and create understanding and awareness among the Company's personnel about personal data protection and related personal data protection laws.

### **3. Manager, Department Head, Supervisor**

Responsibilities: Supervising the collection, use, or disclosure of personal data within its departments, which may have different characteristics for each agency. The duties may be divided as follows:

- Authorize any individuals to access personal information or assign duties to employees to be responsible for taking care of personal information in various parts of the organization.
- Provide guidelines and training on personal data protection in the organization and create mutual understanding on which personal data needs to be collected and which personal data is not required for use within the unit.
- Provide personal data security measures in the agency to meet the standards following the law and this policy.
- Approve the response to the request to exercise the rights of the personal data subject and consult with relevant authorities on such matters, including consultation with the Data Protection Officer or the person responsible for the protection of the Company's personal data, and report to the management for approval if responding to such request may have a significant impact on the Company. Data Subject and/or any other person
- Consult with management and data protection officers to determine appropriate practices.
- Provide records of the collection, use, or disclosure of information by agencies following the list specified in this policy.
- Receive reports from subordinates in case of being notified of the personal data breach and determine whether the breach may pose a risk to affect the rights and freedoms of the personal data subject, including consultation with the Data Protection Officer or the person responsible for personal data protection of the Company and executives to consider any appropriate action orders following this policy.

### **4. Employee**

Responsibilities: Adhering strictly comply with the laws and this Privacy Policy. Especially in procedural areas at the operational level as follows:

- Collect, use, and disclose personal data in compliance with the laws and this policy, including attending training on the protection of the Company's personal data.

- Perform assigned duties in the process of personal data protection including the handling of personal information, such as security, disclosure transmission, or recording of various information, etc.
- Notify supervisors in case where the collection, use, or disclosure of any Personal Data in the Company goes against the law, or when it is deemed that the collection, use, or disclosure of any Personal Data may pose a risk of violation of the rights and fundamental freedoms of the Data Subject.
- Notify the supervisor for approval in case of receiving a request to exercise the rights of the personal data subject.
- Notify supervisors immediately in case of a personal data breach. Whether the breach is caused by the intention or negligence of any person, and whether the breach may or may not pose a risk to the rights and freedoms of the personal data subject.

#### **5. Contractors and service providers who are the Company's personal data processors**

Responsibilities: Following duties and obligations to strictly comply with the law on personal data protection and this policy. It is also subject to the Personal Data Processing Agreement with the Company (if applicable) with the following duties:

- Collect, use, and disclose personal data in accordance with the laws and this policy, including attending training on the protection of the Company's personal data upon request.
- Promptly Notify the Company without delay if there is a personal data breach within 24 hours from becoming aware of the breach.
- Support and assist the Company in responding to requests to exercise the rights of the personal data subject.

Violation of the law and this policy of the employee may be considered as a disciplinary action, and violation of the law or this policy by the contractor or service provider who is the personal data processor of the Company and may also be considered a breach of contract with the Company. If such violation or non-compliance causes damage to the Company. The Company may regard it as grounds for termination of employment or termination of the contract. In addition, there may be criminal penalties, fines, and imprisonment for those acting on behalf of the company who violate or do not comply with the law.

#### **Personal Data Protection Measures**

The Company provides appropriate policy and technical security measures to prevent the unauthorized or unlawful loss, access, use, change, correction, or disclosure of personal data, and reviews such measures when necessary or when technology changes to be effective in maintaining appropriate security following the standards prescribed by law.

### **Recording, Use ,and Disclosure of Personal Data**

The Company shall provide a record of the use and disclosure of collected information with at least as follows:

- Personal data collected, including purposes and retention period
- Use or disclosure of personal data in the case of collecting personal data based on legal bases other than consent
- Rights and methods of access to personal data, including access conditions of the personal data subject
- Refusal or objection to various types of right requests along with reasons as specified in this Policy.
- Description of personal data security measures provided by the Company

These measures are in place to enable the Data Subject to review and enforce the rights as notified or requests to the Company.

### **Sending or transferring personal data abroad or to international organizations**

1. The company can transfer or send personal data to destination countries that have sufficient data protection standards, in accordance with the criteria for data protection set forth by the Data Protection Committee
2. In case the destination country has insufficient standards, The Company can transfer personal data if it meets the legal exemptions as follows:

- Compliance with the law.
- Obtaining consent from the personal data subject who is aware of the inadequate standards of destination country or organization.
- Necessity of the performance of a contract to which the personal data subject is a party, or to take steps as requested before entering into a contract.
- Compliance with agreement of a contract between the Company and individuals or juristic persons for the benefit of the personal data subject.
- Prevention or suppression the danger to life, body, health of the personal data subject or other individuals when the data subject is unable to provide consent at that time.
- It is necessary for the execution of a task carried out in the vital public interest.

3. In case of sending or transferring data between foreign persons or juristic persons belonging to the same entity. The Company may send or transfer personal data between each other without performing the actions set out above. The Company shall establish a Personal Data Protection Policy for the transmission or transfer of data between each other in the same business group that has been audited and certified by the Office of the Personal Data Protection Committee.

**Actions taken in the event of a personal data breach**

When a personal data breach occurs within the Company, where the breach risks affecting the rights and freedoms of the personal data subject, employees and related personnel must coordinate to take legal action, and the Company shall notify the Office of the Personal Data Protection Committee without delay **within 72 hours** from the time of awareness as soon as possible. If the breach poses a high risk of affecting the rights and freedoms of the personal data subject, the Company shall promptly notify the data subject of the breach of the cause and remedy without delay.

**Amendments to the Data Protection Policy**

This Personal Protection Policy may be amended in accordance with changes in laws and business suitability.

**Inquiries and Notification of Personal Data Breach**

In case of any further questions or inquiries regarding personal data protection or request to report a case of personal data breach, please contact:

- Officer responsible for the protection of the Company's personal data
- Irene Enterprise Company Limited
- Address: 22/20 Evergreen View Tower, 2<sup>nd</sup> Floor Soi Bangna-Trad 56, Bangna Tai Subdistrict, Bangna District, Bangkok 10260 Thailand
- Phone number: 02-666 9245,02-666 9241 &02-666 9242
- E-mail: [info@irene-enterprise.com](mailto:info@irene-enterprise.com)