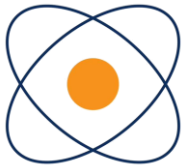

ASTRA

Personal Data Protection Policy

(นโยบายคุ้มครองข้อมูลส่วนบุคคล)

ASTRA

Definitions

Term	Meaning
The Board	The Board of Directors or a delegated committee responsible for overseeing personal data protection.
Data Protection Officer	An individual or group of individuals appointed as the Data Protection Officer or assigned responsibility for personal data protection, or a supervisory body, to comply with the Personal Data Protection Act.
Data Controller	A person or legal entity with the authority to decide on the collection, use, or disclosure of personal data.
Data Processor	A person or legal entity that performs any operation on personal data, including collection, use, or disclosure, on the order or on behalf of the Data Controller. However, such person or legal entity is not the Data Controller.
Data Subject	An individual who is the owner of the personal data and who can be identified or linked to by the data.
Person	A natural person.
Personal Data	Information about a person that makes it possible to identify that person, directly or indirectly, but does not specifically include information of a deceased person.
Processing	Collection, use, or disclosure of data.

Term	Meaning
Sensitive Data	Personal data pertaining to racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or any other data that similarly affects the Data Subject, as defined by the Committee.
Erasure/Destruction	Includes anonymization.
Anonymization	The process of making a dataset that was previously linkable to an individual and identifiable, no longer linkable and identifiable to that individual.

Policy Overview

Introduction

The Company is committed to protecting the personal data received from customers or third parties, especially sensitive data, and to preserve the privacy rights of Data Subjects, and to comply with the Personal Data Protection Act B.E. 2562 (2019) as a Data Controller.

This policy describes the duties, obligations, and procedures for the collection, use, and storage of personal data to comply with the Company's data protection standards, Thai law, and international standards.

The Company's practices will adhere to the following principles:

- The collection, use, and disclosure of data must be in accordance with the announced or specified purposes and be lawful within the limits set by law.
- Personal data shall be processed fairly and lawfully.
- The purpose of processing must be clearly defined and announced.

- Only personal data that is necessary, relevant to the announced or specified purposes, and lawful shall be collected.
- Collected personal data must be accurate and up-to-date.
- Personal data must not be kept longer than necessary.
- Data storage must be protected by appropriate means.

The Company is also responsible for ensuring that personal data is collected and used fairly, stored securely, and not disclosed by unlawful means.

Related Regulations

The Company shall take into account its obligations under relevant anti-money laundering laws, securities and exchange laws, and applicable regulations related to the collection, use, disclosure, and storage of personal data, as appropriate.

Objectives

The purpose of this policy is to serve as a guideline for all Company personnel in the proper processing of personal data, to ensure that all data received from customers and third parties is protected and that necessary security measures are in place to maintain security. This policy is adopted to comply with the aforementioned laws and seeks to instill in the organization a respect for and protection of the privacy rights of the Company's customers and to ensure that all personal data collected is processed according to the general principles of transparency, lawfulness, legitimate purpose, and proportionality.

This Data Privacy Policy ensures that the Company:

1. Operates in compliance with the Personal Data Protection Act B.E. 2562 and best practices.
2. Protects the rights of directors, executives, employees, customers, and partners (if any).
3. Governs how the data of each individual is stored and processed.
4. Protects itself from the risks of personal data breach.

Policy Scope

The responsibility for compliance with this policy and operating procedures lies with the head of each department. The Company should consider appointing a Data Protection Officer to audit the operations in accordance with this policy.

This policy must be reviewed and approved by the Board of Directors before becoming effective, including any material changes to the content of this policy.

Furthermore, the content of this policy should be reviewed regularly to ensure that the Company's policy complies with the law and reduces the risk of non-compliance.

Derogation from Policy

The Data Protection Officer is responsible for overseeing and monitoring the operation in accordance with the established policy and reporting the results of the operation to the Board of Directors according to the meeting schedule of the Board of Directors, or reporting immediately without delay to the Chief Executive Officer for the purpose of correcting defects and mitigating potential damages.

The Company prohibits personnel from failing to comply with or abstaining from complying with this policy, unless there is a necessary reason to abstain from complying with this policy, which must be approved by the Board of Directors only.

Identification of Personal Data

"Personal Data" under the Personal Data Protection Act means information about a person that makes it possible to identify that person, directly or indirectly, but does not specifically include information of a deceased person. Specifically, "Data Subject" means the person to whom the personal data relates.

To explain the term personal data, the Company refers to the National Institutional of Standard and Technology ("NIST") which defines Personal Identifiable Information (PII) as information about an individual that makes it possible to identify that person, directly or indirectly.

The ability to identify a person can be divided into 3 characteristics:

1. **Distinguishability:** Is the capability of the data to distinguish one individual from another. For example, a dataset containing a name, passport number, social security number, or Biometric data can identify the Data Subject. Conversely, if a dataset only contains a credit score, it cannot identify the individual. Additional personal data is required to distinguish the individual.
2. **Traceability:** Is the capability of the data to be used for tracking to identify the specific characteristics of that person. For example, behavior, activities performed by that person, status, or system user action logs that can be used to track the activities of each individual.
3. **Linkability:** Is the capability of the data to be linked and identify the individual, which is divided into 2 types:
    - **Linked Information:** Is the case where data related to different sets of Personal Data Subject, when combined, can identify the Personal Data Subject. For example, two datasets with different PII elements, when a person can access both datasets, they can link the data to identify the Personal Data Subject, including the case of accessing other data related to the Data Subject, if the two databases are in the same system or closely related systems and there is no effective access control. This is considered Linked Information.
    - **Linkable Information:** Is the case where a dataset, if used together with other data, can identify the individual, where the other data to be used together comes from other sources, is not in the same or unrelated systems, and is available on the Internet or other sources. This is considered Linkable Information.

Examples of PII (Personally Identifiable Information) include name, address, email, financial information, health information, criminal records, etc. Unauthorized access, use, or disclosure of PII may cause negative impacts on both the Data Subject, such as being impersonated by a criminal and using the data for some benefit, causing embarrassment, impacting livelihood, or causing financial damage, etc., and causing negative effects on the Data Controller itself, such as affecting the organization's reputation, reducing credibility, or incurring legal liability, etc.

ASTRA

Examples of Personal Data

The following is a list of data that may be considered Personal Data:

• First name, last name, middle name
• National ID number, social security number, passport number, driver's license number, taxpayer identification number, bank account number, credit card number
• Email address, telephone number
• Device information such as IP address, MAC address, Cookie ID
• Unique characteristic information such as facial image
• Biometric data, which is Sensitive Personal Data, such as facial model data, fingerprint model data, X-ray films, iris scan data, voice identity data, genetic data, etc.
• Data identifying a person's property such as asset tag number, information about a person linked or linkable to one of the above, such as date of birth, place of birth, weight, height, geographical location data
• Race, religion, belief, cult, ethnic origin, philosophy, sexual behavior, political opinions, criminal records

Examples of Non-Personal Data

The following is a list of data that is not considered Personal Data:

• Company registration information, business contact information that does not identify an individual, such as office address, company email, office telephone number, office fax number
• Information that cannot identify an individual, such as Anonymized Data
• Information of a deceased person

Applicability of this Policy

This privacy policy applies to all data collected by the Company, especially identifiable personal data that the Company possesses and can link to the Data Subject, which may include, but is not limited to, the following data:

1. KYC data, including name, address, transaction data, etc.
2. EDD data, including financial status, financial documents, etc.
3. Contract data from service agreements, employment agreements, etc.
4. Personal data received through customer service.
5. Any other data related to an individual.

All employees of the Company, regardless of the type of employment, whether labor or contract for hire, must comply with the requirements set forth in this policy.

Potential Risks of Non-Compliance

This policy helps protect the Company from critical data security risks, including:

1. **Breach of Confidentiality:** In the case of inappropriate disclosure of information or violation of confidentiality agreements.

2. **Damage to Reputation:** Including failure to prevent unauthorized access to personal and/or sensitive data by third parties.
3. **Security Breach:** In the case of unintentional, unlawful, or unauthorized use, interference, or disruption of operation or unavailability of personal data.

General Personnel Practices

1. Access to personal data must be strictly based on the principle of *need-to-know* to perform duties.
2. Data should not be disclosed through informal means, such as social media (including messaging apps) or physical data transfer, except when necessary and with sufficient measures to maintain confidentiality.
3. The Company shall provide training to all personnel to understand their responsibilities in data processing and build a basic understanding of this policy.
4. Employees should keep all data secure by using reasonable safeguards and following the guidelines established by the Company.
5. Personnel must use strong passwords in accordance with the Company's security practices and international best practices, and should not disclose such passwords.
6. Personal data should not be disclosed to unauthorized persons, either within or outside the Company.
7. Data should be reviewed and updated regularly. If no longer necessary, it should be erased and disposed of according to the time frame specified by law.
8. Personnel must seek assistance from their supervisor and/or the Data Protection Officer if they are unsure about the processing of personal data to be collected, used, or disclosed.
9. All personnel involved in the processing of personal data must operate and maintain personal data under strict confidentiality measures. In cases where personal data is not intended for public disclosure, these duties remain binding even if the personnel leaves the Company, transfers to another position, or upon termination of employment or the contractual relationship.

ASTRA

Personal Data Processing - Data Collection

The Company collects data to be able to fulfill its obligations to the Data Subject. The Company focuses on secure and efficient data storage, and compliance with applicable laws and regulations.

The Company will not collect, use, and/or disclose personal data in all cases, except for the legal exceptions specified in the Personal Data Protection Act, which include:

1. **Research Basis:** To achieve purposes related to the preparation of historical documents or archives for the public interest, or for research or statistical purposes, with appropriate measures established to protect the rights and freedoms of the Data Subject, and in accordance with the announced regulations set by the Committee.
2. **Basis of Vital Interest:** To prevent or suppress danger to the life, body, or health of a person.
3. **Contractual Basis:** To fulfill a contract to which the Data Subject is a party, or to take steps at the request of the Data Subject prior to entering into a contract.
4. **Legitimate Interest Basis:** Provided that such interests are not overridden by the fundamental rights of the Data Subject in that personal data.
5. **Public Interest Basis:** To perform tasks carried out by the Data Controller for the public interest.
6. **Legal Basis:** To comply with the law to which the Data Controller is subject.
7. **Data Subject's Consent Basis**

To simplify operations, the Company should make every effort to avoid using the consent basis as it is the most burdensome basis for the Company.

Furthermore, the Company must prepare a privacy policy before or at the time of data collection, which must contain the following:

1. The purpose of collecting the personal data for use or disclosure.
2. Informing the Data Subject of the legal basis, in cases where the Data Subject must provide their personal data to comply with that legal basis, including informing of potential consequences if the Data Subject does not provide such personal data.
3. The personal data to be collected and the retention period for the personal data. If the

retention period cannot be specified, the expected retention period must be stated according to the standard data retention period.

4. The type of person or entity to whom the collected personal data may be disclosed.
5. The contact information and details of the Data Controller.
6. The rights of the Data Subject as specified in the Personal Data Protection Act.

Sensitive Data

The following items are considered sensitive data:

• Race, ethnic origin, marital status, age, skin color, and religion, philosophical or political affiliation
• Health, disability, education, genetics, biometrics, sexual behavior data, criminal records
• Social security number, health information, license, tax return, trade union information
• Or any data that may similarly affect the Data Subject as prescribed by the Office of the Personal Data Protection Committee

The Company will collect the Data Subject's sensitive data only with the consent of the Data Subject, unless a legal exception applies.

Company employees should access and/or process sensitive data only when:

- The legitimate purpose for such action is clearly documented.
- Consent has been obtained from each Data Subject, and
- Protective measures are used to ensure that only authorized individuals can access the personal data.

Incapacitated Persons

In the case where the Company processes the data of an incapacitated person, the Company must obtain consent from the legal representative before proceeding with data processing.

Data Collection

The Company may collect, use, process, and examine personal data of customers, employees, partners, shareholders, and/or applicants when:

- It is for the provision of the Company's services and for timely and efficient customer support.
- Processing transactions and sending notices about customer transactions.
- Resolving disputes, collecting fees, and troubleshooting.
- Preventing activities that may be prohibited or illegal.
- Customizing, measuring, and improving the Company's services, as well as the content and layout of the Company's websites and applications.
- Sending direct marketing, service update notifications, and promotional offers.
- Comparing data for accuracy and verifying with third parties.
- Monitoring network quality and security and training our employees.
- Other related services provided by the Company.

The types of personal data the Company collects depend on the nature of the relationship and/or transaction considered, including but not limited to:

1. First name, last name, gender, place, and date of birth.
2. Temporary/permanent residential address.
3. Copy of National ID card, passport, social security number.
4. Employment or business information.
5. Payment details, including credit card information and bank details.
6. Contact details, including telephone number and email address.

7. Latest income documents.
8. Proof of latest billing address (if any).
9. Other necessary information.

The Company may collect data about the Data Subject, including but not limited to transactions, account history, and inquiries about products and services, which the Company collects as authorized or required by law.

The Company may collect data about the Data Subject when necessary or permitted by law. For example, the Company may require personal data to verify the identity of the Data Subject under relevant anti-money laundering policies and applicable laws.The Company may collect data from other sources and when supported by a legal basis through:

- Contact and communication with our customer contact department. To answer the Data Subject's questions, the Company and its representatives may ask for their name, contact number, and email address.
- Sharing the Data Subject's personal data with service providers or third parties, with the customer's consent.

Personal Data Processing - Data Usage

The Company remains subject to compliance with the use of personal data according to legal criteria and the legal bases mentioned above in this policy. The purposes of data use may include, but are not limited to:

- To comply with laws and regulations (for KYC or customer identification).
- To fulfill our obligations arising from contracts made between the Company and the customer.
- To conduct our day-to-day business purposes (to process transactions, applications, and Data Subject requests, etc.).

Use of Personal Data for Original Purposes

The Company has the right to store, collect, use, and disclose personal data that the Company received

from the Data Subject before the relevant part of the Personal Data Protection Act came into effect, and can continue to operate for the original purposes. If the Data Subject does not wish for the Company to continue storing, collecting, using, or disclosing the received personal data, the Data Subject can notify the Company to withdraw consent at any time through the channels specified by the Company, unless the storage, collection, use, or disclosure is required by law.

Marketing Use

In the event that the Company offers products and services under the Data Subject's consent for the processing of the Data Subject's personal data, the Company may process the data for marketing purposes, and the Company can also use the Data Subject's data to:

- Group service usage to offer special privileges;
- Conduct market research;
- Offer marketing services and promotional materials.

Such marketing activities may be by post, telephone, SMS, email, or any other electronic means. The Data Subject can notify the Company at any time if they no longer wish to receive direct marketing offers (opt-out), which is stated in the section on Data Subject rights in the next topic of this policy.

Data Processing - Disclosure and Sharing

The Company will not share the Data Subject's personal data with third parties for direct marketing purposes, unless the Data Subject provides specific consent.

The Company may share the Data Subject's personal data with third parties for other purposes, only in the following situations:

1. For processing payments/services, the Company may securely share personal data with individuals or companies that are parties to the transaction, which may include the Data Subject's contact information, registration date, amount of payment received. This data will be shared for transaction purposes only.
2. Contracted service providers who assist in the Company's business operations, such as fraud prevention, billing, marketing, KYC services (Idp, AS, RP), and technology services.

3. Financial institutions with which the Company is partnered and/or collaborates.
4. A company that merges with or is acquired by the Company (If such a merger occurs, the Company shall require the new merged entity to comply with this privacy policy with respect to the Data Subject's personal data. All Data Subjects will be notified in advance if there are changes in the relevant policy).
5. Law enforcement by government officials or third parties when:
    - The Company is compelled to do so by a subpoena, court order, or similar legal process, or
    - The Company believes in good faith that the disclosure of personal data is necessary to prevent physical harm or financial loss.
    - The Company reports suspicious illegal activities or to investigate violations of contractual or service agreements.
    - A third party has received consent from the Data Subject or is ordered to do so.
6. Any other case supported by a legal basis.

The Company will not sell or rent the Data Subject's personal data to third parties for marketing purposes, and will share personal data with third parties only as described in this policy.

To mitigate the risk of unlawful disclosure of personal data, the Company has a procedure for requesting the disclosure of personal data.

Data Storage and Security Measures

1. **Data Storage Format:** The Company may collect and store personal data in both digital/electronic format and in paper/physical format.
2. The Company will maintain secure electronic data storage systems in accordance with IT best practices to preserve data security and privacy, and implement data encryption. In the case of physical document storage, it should be stored with restricted access measures.
3. The Company will endeavor to maintain state-of-the-art security for data storage, ensuring that retention is only within the timeframe prescribed by law.
4. Security systems shall comply with the best standards established in related policies.

ASTRA

Data Access

Security Measures:

The Company will use appropriate security measures to protect the Data Subject's personal data from unauthorized access or unauthorized alteration, disclosure, or destruction. These measures include internal monitoring of data collection, storage, and processing practices, as well as physical security measures to prevent unauthorized access.

Organizational Framework

The Company will implement appropriate and effective measures in a timely manner to prevent the unauthorized disclosure, erasure, or modification of personal data in its possession. The Company will use physical and technical measures to protect personal data. These actions are aimed at maintaining the availability, integrity, and confidentiality of personal data and protecting the data from potential natural disasters, accidental loss or destruction, or human dangers such as unlawful access, misuse, fraud, unlawful destruction, data alteration, and others.

Responsible Personnel

The Company defines the roles, duties, and responsibilities related to compliance with the policy and the Personal Data Protection Act as follows:

1. **The Board of Directors:** Has the duty to oversee the Company's compliance with the relevant Personal Data Protection law through the Company's supervisory authority, and also has the duty to approve policies related to personal data protection and oversee the establishment of sufficient regulations, procedures, and operation manuals to enable personnel to comply with the Personal Data Protection law.
2. **Supervisory Authority:** Has the duty to oversee that all Company personnel strictly comply with this policy and to ensure that each department related to personal data establishes operating guidelines to comply with this policy, as well as providing consultation on rules and operating guidelines that comply with the law and policy, conducting training for Company personnel, and jointly preparing data on records of processing activities, privacy policy announcements, risk assessments, and any other activities to comply with the law and this

policy, and storing them as evidence for relevant internal and external supervisory authorities to audit.

3. **Departments Related to Personal Data:** Have the duty to give importance to and strictly comply with the law and this policy, by establishing regulations and operating procedures to enable compliance with the law and this policy, as well as establishing information technology systems or making contracts with external parties to comply with the requirements of the law and this policy.

4. **Data Protection Officer (DPO):** In the event that the Company appoints a Data Protection Officer as deemed appropriate by the Board of Directors, the Data Protection Officer, in collaboration with the Compliance and Audit Officer, will oversee compliance with the Personal Data Protection Act and related organizational policies as follows:

    - Providing advice to the Company, including employees or service providers of the Company, regarding compliance with the Personal Data Protection Act.
    - Auditing the operations of the Company, including employees or service providers of the Company, regarding the collection, use, or disclosure of personal data to comply with the Personal Data Protection Act.
    - Coordinating and cooperating with the Committee in the event of problems in the collection, use, or disclosure of personal data of the Company, including employees or service providers of the Company, in relation to the Personal Data Protection Act.
    - Reporting progress to senior management regarding data protection responsibilities, risks, and issues.
    - Conducting privacy impact assessments and taking necessary steps to mitigate and manage risks.
    - Reviewing all data protection procedures and related policies as scheduled.
    - Providing data protection training and guidance for individuals subject to this policy.
    - Responding to requests from individuals to view data held by the Company.
    - Answering questions and managing the Data Subject's rights exercise procedures.
    - Reviewing and approving commercial agreements or data sharing agreements with third parties.

- Effectively implementing security measures, security incidents, and data breach protocols, and managing the notification and reporting process to the Office of the Personal Data Protection Committee.
- Other responsibilities specified in related policies.

The Data Protection Officer must maintain the confidentiality of personal data known or obtained during the performance of duties under this policy.

Duty of Confidentiality

All employees will be asked to sign a Non-Disclosure Agreement (NDA) as part of their employment contract, along with an employee liability agreement regarding data protection policy violations, to ensure that the Company can claim liability against the employee according to law, in the event that the Company is liable for the actions of the employee.

All employees who access personal data must operate and maintain personal data under strict confidentiality. If such data is not intended for public disclosure, this duty of confidentiality shall remain in effect upon transfer to another department, team, position, or even after the termination of the employment relationship.

Testing, Evaluation, and Effectiveness Assessment of Security Measures

The Company will regularly review its security policy, conduct vulnerability assessments, and perform penetration tests within the Company according to the Company's IT and security policies. Third parties may be hired to complete such assessment tests. Any defects and recommendations must be communicated to the Data Protection Officer and rectified promptly.

Data Recording and Internal Audit

The Company must maintain at least the following records so that the Data Subject and the Office of the Personal Data Protection Committee can audit them, which may be in written or electronic form:

1. Personal data collected;
2. The purpose of collecting each type of personal data;

3. Details of the Data Controller;
4. The retention period of personal data;
5. Rights and methods of access to personal data, including conditions regarding individuals who have the right to access personal data and the conditions for accessing such personal data;
6. The use or disclosure of personal data in cases where the Company uses or discloses personal data in accordance with the law without requiring consent;
7. The denial of requests or objections mentioned in the Data Subject's rights section.

The Data Protection Officer must conduct ongoing internal audits in accordance with this Company policy and report the results of the audit directly to the Board of Directors.

Data Retention and Disposal Procedures

The Company will retain the customer's personal data as long as the customer's account remains active. All customer identification data must be securely retained as long as the account exists until the business relationship between the Company has ended, after which the Company can no longer claim a contractual basis for the use, collection, or disclosure of data of a customer whose account has been deactivated.

However, in accordance with the Anti-Money Laundering Act B.E. 2542 (1999), the Company is under a legal obligation to retain the following customer data after the termination of the business relationship:

- All transaction records and documents of the Company's customers must be kept and securely stored for five (5) years from the date of the transaction, unless there is a necessary and reasonable matter notified in writing by the Secretary-General.

- When a customer's account is closed, the Company will securely store all customer identification records and transaction documents related to the CDD and EDD processes for at least ten (10) years from the date of closure, unless there is a necessary and reasonable matter notified in writing by the Secretary-General.

Upon the expiration of the above periods, physical and electronic copies of all personal data will be destroyed and disposed of using secure technology.

ASTRA

Data Security Breach Incident

The Company will take steps to correct and manage data breaches to comply with the Company's security policy.

Data Breach Response Working Group

The Data Breach Response Working Group shall be responsible for any action to respond to an incident promptly. In the event of a personal data breach, the Working Group must conduct a preliminary assessment of the incident or breach to confirm the nature and scope of such incident. In addition, measures must be provided to mitigate and control the impact of the incident.

The Data Breach Response Working Group will consist of the following employees/officials:

- IT Security Officer
- Data Protection Officer

The Working Group is also responsible for notifying senior management of security breaches and related security incidents, and notifying affected Data Subjects of the incident, including notifying the Office of the Personal Data Protection Committee within the 72-hour period required by law.

The Working Group must prepare detailed documentation of the incidents found, including an annual report to submit to the executives for acknowledgment.

In the case where the personal data breach is caused by an external service provider of the Company, the Company requires the external service provider to notify the Company in writing or through the Company's email channels within 24 hours from the time the external service provider becomes aware of the personal data breach, so that the Company can assess and notify the relevant authorities as required by law.

Preventative Measures against Security Incidents

The Company must conduct risk assessments periodically to identify potential risks in the data processing system and disclose vulnerabilities to data security breaches. In addition, the security department must periodically audit employee compliance with the security policy to minimize risks.

Personal Data Backup and Recovery Procedures

The organization will always maintain backup files for all personal data under its care. In the event of a security incident or data breach, the organization will always compare the backup data with the affected files to check for discrepancies or changes resulting from the incident.

Data Accuracy

The Company must take all appropriate steps to ensure that personal data is kept accurate and up-to-date. The Company must ensure that Data Subjects have the opportunity to correct their personal data. The Company must record details of such changes and keep them for audit purposes.

The Company will ensure that personal data is current and not altered, unless with the customer's consent:

1. Data will be stored and copied in the safest place and only as many copies as necessary. Personnel should not create unnecessary additional copies of datasets.
2. Personnel should use every opportunity to ensure data is up-to-date, such as confirming customer details when they call.
3. The Company will facilitate the Data Subject in updating the data held by the Company, such as through the Company's website or customer service system.
4. Data should be updated when inaccuracies are found, for example, if a customer cannot be contacted with the stored phone number, a way should be found to remove it from the database when it is no longer necessary to use it.

Data Subject Rights, Inquiries, and Complaints

All Data Subjects have rights over their own data as prescribed by law, and the Company will guarantee those rights so that the Data Subject can exercise them. The Data Subject has the following rights:

- **Right of Access:** The Data Subject has the right to access personal data under the responsibility of the Company by requesting the Company to provide a copy of such data to the Data Subject and requesting the Company to disclose data related to the Data Subject.

- **Right to Rectification:** The right to correct the Data Subject's personal data to be current, complete, and not misleading.
- **Right to Data Portability:** The right for the Data Subject to transfer their personal data if the Company organizes such personal data in a format that is readable or usable automatically and can be processed or disclosed by automated means.
- **Right to Object:** The right for the Data Subject to object to the collection, use, and/or disclosure of the Data Subject's personal data at any time if such action is carried out for legitimate interests.
- **Right to Erasure or Destruction:** The right for the Data Subject to request the erasure, destruction, or anonymization of the Data Subject's personal data according to legal requirements.
- **Right to Restriction of Processing:** The right for the Data Subject to request the restriction of the processing of the Data Subject's personal data according to legal requirements.
- **Right to Withdraw Consent:** The right for the Data Subject to withdraw such consent at any time under legal requirements.

The Company provides channels for the Data Subject to exercise these rights by sending their request to the Data Protection Officer to respond to the exercise of such rights. The Data Protection Officer will verify the identity of the person exercising the right before granting any right. The Company may prepare a standard request form for the Personal Data Subject to make a request. The Data Protection Officer must proceed with the request within 7 to 30 working days, depending on the complexity of granting the right.

This policy shall be effective from February 26, 2026, onwards.

Mr. Chatchaval Jiaravanon

Chairman of ASTRA Enterprise

Public Company Limited

Appendix A.

Operating Procedure upon Discovery of Personal Data Leak