Public	
Notification	
Personal Data Protection Policy	Dated: 26/05/2022 Version: 001/2022
	Lasted Verification Date: 26/05/2022
Issued by: Ms. Maneewan Mukdaphongsathon and Ms. Ampika Jaroenchai	
Verified by: Mr. Rapeepong Limwongthong	
Approved by: Mr. Thiraphong Chansiri and Mr. Shue Chung Chan	
Distribution List: All Thai Union Colleagues in Thailand	
Targeted Group: Department Manager of All Thai Union Entities in Thailand	
Distribution Method: Online Communication	

List of contents

Personal Data Protection Policy

1. Introduction

As many countries had started to develop and enact their own data protection laws after the enforcement of General Data Protection Regulation (GDPR) in 2018, the law on data protection is common in every country in the world.

Thai Union Group Public Company Limited is a global seafood leading company which focusing on sustainability and aims to satisfy our customers with quality products. In order to comply with any relevant law and regulation on data protection (including but not limited to the Personal Data Protection Act of Thailand ("**PDPA**")) and to protect Personal Data of our stakeholders including but not limited to our customers and employees from unauthorized use and unlawful loss, we therefore establish this Personal Data Protection Policy ("**Policy**") to implement appropriate procedures of collection, use and disclosure of Personal Data.

This Policy covers the information of persons whom we have collected, used or disclosed their Personal Data.

2. Purpose

This Policy sets out mandatory requirements for Thai Union Group Public Company Limited and all its subsidiaries and affiliates in Thailand (collectively or separately referred to as "**Thai Union**") in order to ensure that all Personal Data shall be;

a. processed lawfully and in a transparent manner in relation to the Data Subject;
b. collected for specified, explicit and other legitimate purposes and not processed in a manner that is incompatible with these purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; and
e. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organizational measures.

All CEOs or Managing Directors, Management and Employees shall be aware that they must ensure the confidentiality, integrity and availability of all Personal Data, as required.

This Policy and the related documents shall be reviewed from time to time, or whenever the applicable law or the business environment of Thai Union changes in a way that affects the current Policy.

3. Definitions

For purposes of this Policy, the terms set forth below shall have the meanings specified as follows;

Board of Directors means Directors of Thai Union.

CEO or Managing Director means CEO, Managing Director or the highest management position in Thai Union.

Cookie means a unique file which created by a website and stored on computer or a user's communication device which stores the user's Personal Data, usage and other settings for improving the experience of website's user.

Data Administrator means any person who has been appointed by the Management of each Department/ Shared Service Unit/ Business Unit to manage and monitor all relevant processes including having authority to categorise, monitor and manage Personal Data in order to align with this Policy and other relevant policies, Procedures and Departmental Procedures e.g. Thai

Union's Information Classification Schema. Data Administrator also has authority to assign and revoke Employees' right to access Personal Data.

Data Controller means a person who decides to collect, use and disclose any Personal Data of the Data Subject.

Data Processor means a natural or legal person, public authority, agency or any other body who processes on a collection, use and disclosure of Personal Data on behalf or under the name of the Data Controller. Data Processor shall include all of its Sub-Processors.

Data Protection Impact Assessment (**DPIA**) means a process designed to describe the processing, assess its necessity and proportionality and manage the risks to the rights and freedoms of Data Subject resulting from the processing of Personal Data by assessing them and determining the measures to address them.

Data Protection Officer (**DPO**) means a person or persons appointed under this Policy to perform the duties of DPO as required by PDPA or any other relevant regulation and to be responsible for advising and auditing operations of the Data Controller or the Data Processor to comply with PDPA.

Data Subject means an identifiable natural person by the Personal Data.

Departmental Procedure means any Department Procedure issued and announced by any relevant Department/ Shared Service Unit/ Business Unit who related to the Personal Data.

DPA means data processing agreement.

DSA means data sharing agreement.

Employee means all employees of Thai Union.

Management means the Management of Departments /Shared Service Units/ Business Units under Thai Union.

NDA means non-disclosure agreement.

Office means the Office of the Personal Data Protection Committee.

PDPA means the Personal Data Protection Act of Thailand including its regulations, notifications and rules.

Personal Data means any Personal Data that can identify a person whether directly or indirectly but not includes information of dead person.

Policy means this Personal Data Protection Policy.

Privacy Notice means a document that inform the Data Subject on how Thai Union gathers, uses, discloses and manages their Personal Data.

Procedure means any Procedure issued to clarify operational details for implementation of this Policy.

Sensitive Personal Data means Personal Data that is sensitive and prohibited for collecting without the express consent from the Data Subject. This includes Personal Data pertaining to: nationality, lineage, skin color, political opinion, religion, sexual behavior, criminal history, health information, disability, labor union information, genetic information, biological data, and other Personal Data pursuant to PDPA.

Sub-Processor means any third party engaged by the Processor for carrying out processing activities in respect of the Personal Data on behalf of the Data Processor.

Thai Union means Thai Union Group Public Company Limited and all of its subsidiaries and affiliates in Thailand.

Third Party means natural or juristic person other than the Data Subject or the Data Controller who is a recipient or processor of personal data.

4. Duty and Responsibility

4.1 Board of Directors

4.1.1 Review and approve the Policy.

4.1.2 Regulate and ensure that the Policy and relevant Procedures are fully complied and implemented in Thai Union.

4.2 CEO or Managing Director

4.2.1 Appoint DPO for each entity to perform DPO's duties according to PDPA and this Policy.

4.2.2 Monitor and ensure that the Policy and relevant Procedures are fully complied and implemented in the concerned entity under Thai Union.

4.3 Management

4.3.1 Ensure that the concerned Department /Shared Service Unit/ Business Unit complies with PDPA and this Policy, and the Management of Department/ Shared Service Unit/ Business Unit involving with the Personal Data of:

a) customers, including their directors, representatives, authorized persons or other persons working on behalf the customers;

b) business partners including their directors, representatives, authorized representatives or other persons working on behalf of the business partners;

c) job applicants, internship applicants and interns;

d) Employees, trainees and family members;

e) shareholders and directors;

f) visitors and event participants; and/or

g) other persons whom the Department/ Shared Service Unit/ Business Unit have collected, used or disclosed their Personal Data;

shall issue and announce detailed Departmental Procedure (as explained in Section 9) for its daily operation.

4.3.2 Designate a responsible person to perform the duties of Data Administration (as explained in Section 4.6) of this Policy.

4.3.3 Ensure that Data Subject has been informed and acknowledged the purpose of collection, use and disclosure of Personal Data and the rights of Data Subject, e.g. sharing of the relevant Privacy Notice before or while collecting, using or disclosing Personal Data. Please see Template of Privacy Notice in Appendix No.1.

4.3.4 Ensure that the collection, use and disclosure of the Personal Data are aligned with the purpose as informed to the Data Subject or the consent received. In case that a consent is required, the Management is required to ensure that the Data Subject gives a consent in accordance with this Policy, Procedures and Departmental Procedure.

4.3.5 Promptly inform DPO in case of data breaches and work closely with DPO.

4.3.6 Provide instruction to Data Administrator to execute the request for the exercise of rights of Data Subject, for example, to correct, erase or delete, destroy or anonymize the Personal Data according to the Data Subject's request and to record and retain record of such transactions.

4.3.7 Appoint at least one Data Administrator to manage and monitor Personal Data collected, used and processed by such Department/ Shared Service Unit/ Business Unit.

4.3.8 Oversee, monitor and ensure that Data Administration performs its duties in compliance with this Policy, Procedures and Departmental Procedure.

4.3.9 Organize awareness-raising activities and trainings regarding related Personal Data processing.

4.4 Data Protection Officer

4.4.1 Provide advices to the Data Controller or the Data Processor and the Employees of the Data Controller or of the Data Processor in compliance with PDPA and this Policy.

4.4.2 Investigate the performance of the Data Controller or the Data Processor and the Employees of the Data Controller or of the Data Processor with respect to the collection, use, or disclosure of the Personal Data in compliance with PDPA and this Policy.

4.4.3 Coordinate and cooperate with the Office in the circumstance where there is any incident with respect to the collection, use, or disclosure of the Personal Data undertaken by the Data Controller or the Data Processor, including the Employees of the Data Controller or of the Data Processor including Third Party.

4.4.4 Keep confidentiality of the Personal Data known or acquired in the course of the performance of DPO's duties under PDPA and this Policy.

The Data Controller or the Data Processor shall support the Data Protection Officer in performing the tasks by providing adequate tools or equipment and facilitating the access to the Personal Data in order to perform the duties.

The Data Protection Officer may perform other duties but the Data Controller or the Data Processor must warrant to the Office that such duties or tasks are not against or contrary to the performance of the duties under the PDPA.

4.5 Employee

4.5.1 Ensure and being responsible that the process for collection, use and disclosure (including but not limited to the process for data classification, data processing, data storage, data transmission, data disposal, and data destruction) of Personal Data are in compliance with the PDPA, this Policy, Procedures and Departmental Procedures.

4.5.2 Notify the DPO immediately of any Personal Data breach or incident.

4.5.3 Inform the DPO and CEO or Managing Director or report through Thai Union's reporting channels immediately of any action that may be violated of the PDPA or this Policy.

4.6 Data Administrator

4.6.1 Ensure that the collection, use, disclosure and processing of Personal Data by Employees in the Department/ Shared Service Unit/ Business Unit are in compliance with the PDPA, the Policy, Procedures and Departmental Procedures.

4.6.2 Record the list of Employees who can access to Personal Data and the Employees' use of the Personal Data.

4.6.3 Record the list of Data Processors and any other Third Party receiving the Personal Data from Thai Union.

4.6.4 Ensure that NDA and DPA have been completely signed according to Section 5.7.

4.6.5 Handle the requests made by the Data Subject in order to manage the Personal Data according to the PDPA, this Policy, Procedures and Departmental Procedure.

4.6.6 Ensure that the Personal Data has been classified according to Thai Union's Information Classification Schema.

5. Personal Data Protection

5.1 Classification

Personal Data shall be classified in accordance with Thai Union's Information Classification Schema regulated in Thai Union's Information Security Policy and Personally Identifiable Information (PII) – Reference Document taking into account its value, legal requirements, sensitivity, and criticality to Thai Union. Thai Union's guideline for Personal Data classification will be further issued by the Group Information Technology Department. Personal Data shall be securely processed, stored, transmitted, disposed, and destroyed by assigned Employees in accordance with its classification level and shall be handled in accordance with Thai Union's Information Classification Schema.

Employees are responsible for defining the classification level in accordance with Thai Union's Information Classification Schema of data under Employees' responsibility and to ensure that the receivers are aware of the classification level by means of, e.g., labelling, email, etc.

5.2 Collection

5.2.1 The collection shall be limited to the extent necessary in relation the relevant purposes as determined by Thai Union, under the consent of Data Subject or in accordance with the rules prescribed by PDPA, for example, (1) for contract performing or requested by Data Subject, (2) for legal obligations, (3) for legitimate interest, (4) for public interest and/or (5) for preventing a danger to a person's life, body or health.

5.2.2 The Data Subject shall be informed of the following details.

a. the purpose of the collection

b. notification of the case where the Data Subject must provide

c. period of collection

d. the categories of persons or entities to whom the collected Personal Data may be disclosed

e. information, address, and the contact details of the Data Controller

f. rights of the Data Subject

g. the option for the Data Subject to withdraw consent

5.3 Use

5.3.1 Use and processing of Personal Data shall be based on the PDPA, this Policy, Procedures and Departmental Procedures. In addition, using and processing of the Sensitive Personal Data must be taken with extra security.

5.3.2 When processing Personal Data, Employees shall record the following details to enable the Data Subject to check upon:

a. the collected Personal Data;

b. the purpose of the processing and use of the Personal Data in each category;

c. details of the Data Controller;

d. the retention period of the Personal Data;

e. rights and methods for accessing to the Personal Data, including the conditions regarding the person having the right to access the Personal Data and the conditions to access such Personal Data;

f. the use or processing of the Personal Data; and

g. the rejection of request to exercise rights of the Data Subject.

5.4 Disclosure

5.4.1 Employees and Third Party shall not disclose any Personal Data beyond the informed objectives or the Data Subject's consent except required or allowed by the PDPA.

5.5 Storage

The electronic Personal Data shall be securely stored in accordance with the PDPA and Thai Union's Information Classification Schema on cloud, applications or other secured systems approved by the Group Information Technology Department.

In addition, Personal Data in non-electronic format shall be stored in secured storage, and accession to such storage shall be limited with appropriate security according to relevant Departmental Procedure in order to avoid unauthorized accession of Personal Data.

Where the Data Subject's consent is obtained, Employees shall store such consent together with the Personal Data in the same systems and/or storage.

5.6 Transfer

Personal Data may be transferred between Employees within Thai Union only when necessary for performance of work and restricted for informed business purposes in accordance with the PDPA, this Policy, Procedure and Departmental Procedure.

5.7 Data Processor / Third Party

5.7.1 If any Employee needs to transfer the Personal Data to any Data Processor outside Thai Union, or the Personal Data has to be collected, used and/or processed by any Data Processor or destroyed by any, the Employee shall arrange the Data Processor to sign the NDA the DPA using Thai Union's templates or the NDA and the DPA which have been reviewed by the Legal Department, and shall ensure that the Data Processor has adequate data protection security and standard.

If it is required by the PDPA to appoint a representative of the Data Processor in Thailand, the relevant Employee and Data Administrator shall ensure the compliance of the Data Processor before engaging the Data Processor. This is also applied in case that the Data Processor is related person.

In case of any deviation of the NDA or the DPA from Thai Union's standard, a request shall be documented by relevant Employee, which will be reviewed and approved by the relevant Management and the Legal Department. All approvals in this regard will be based on the level of potential risk and security standard of the Data Processor.

5.7.2 If any Employee needs to share the Personal Data to Third Party outside Thai Union, the Employee shall arrange Third Party to sign the DSA using Thai Union's templates or the DSA which have been reviewed by the Legal Department, and shall ensure that the Data Processor has adequate data protection security and standard.

5.8 Update and Accuracy

Employees and Data Administrators shall promptly take reasonable steps to ensure Personal Data is accurate and up to date in accordance with the request of Data Subject.

When the Data Subjects request to withdraw their consent, the relevant Employee and Data Administrator shall consult with the Management and take necessary actions to ensure that the request to withdraw has been properly handled according to the PDPA, this Policy, Procedure and Departmental Procedure.

The relevant Employee and Data Administrator shall response to Data Subject's requests within 30 (thirty) days and strictly follow Policy, Procedure and other relevant Departmental Procedures.

5.9 Erasure and Destruction

Retention period of Personal Data shall be aligned with the relevant Departmental Procedure. However, in all circumstances, Personal Data shall not be retained for more than 10 (ten) years.

Employees and Data Administrators shall erase and destroy Personal Data when the Personal Data is no longer necessary or when the retention period expires in a secure manner according to the relevant Departmental Procedure.

5.10 Security Measures

5.10.1 Group Information Technology Department must ensure that Thai Union has sufficient security measures (the measures should cover all relevant security areas including but not limited to software, hardware, system and application) to protect electronic Personal Data according to international standards and the PDPA.

5.10.2 All relevant Departments /Shared Service Units/ Business Units shall issue and announce security measures guidelines for non-electronic Personal Data collected, used, transferred, disclosed, processed, retained and destroyed by such Department /Shared Service Unit/ Business Unit.

5.10.3 Employee and Data Administrator shall strictly comply with Thai Union's Information Classification Scheme regulated in Thai Union's Information Security Policy and the relevant Departmental Procedure.

6. Audit Measures

6.1 All relevant Departments/ Shared Service Units/ Business Units shall ensure Personal Data activities updated and correct including review of Personal Data's collection, use, storage, retention period, security and breach from time to time.

6.2 Risk Management Department shall evaluate the DPIA for all relevant Departments/ Shared Service Units/ Business Units in aspect of data privacy risk which is likely to result in a high risk to the Data Subject's rights, and to identify any additional necessary measures to mitigate such risks.

6.3 Internal Audit Department who is third line of defense shall randomly check the implemented controls of security and data protection which will be conducted base on annual risk assessment to assure the compliance of this policy and PDPA requirements.

7. Data Subject's Right

7.1 Right to Withdraw Consent

For the purposes the Data Subjects have consented to the collection, use and/or disclosure of Personal Data, Data Subjects may have the right to withdraw consent at any time.

7.2 Right to Access

Data Subjects may have the right to access or request a copy of the Personal Data which Thai Union has been collecting, using and/or disclosing. For privacy and security, Thai Union may require proof of the Data Subject's identity before providing the requested Personal Data.

7.3 Right to Data Portability

Data Subjects may have the right to obtain Personal Data in a structured, electronic format, and to transmit such Personal Data to another Data Controller, where (a) the Data Subjects have provided the Personal Data to Thai Union, and (b) Thai Union has been collecting, using and/or disclosing that Personal Data on the basis of Data Subject's consent or other legitimate purposes.

7.4 Right to Object

Data Subjects may have the right to object to certain collection, use and/or disclosure of Personal Data.

7.5 Right to Erasure

Data Subjects may have the right to request Thai Union to delete, destroy or anonymize Personal Data that Thai Union has been collecting, using, and/or disclosing, except that Thai Union is not obligated to do so if Thai Union needs to retain such Personal Data in order to comply with a legal obligation or to establish, exercise or defend legal claims.

7.6 Right to Restriction

Data Subjects may have the right to restrict the use of Personal Data when the Data Subject believes such Personal Data is inaccurate, that our collection, use and/or disclosure is unlawful, or that Thai Union no longer needs such Personal Data for a particular purpose.

7.7 Right to Rectification

Data Subjects may have the right to request for rectification of any incomplete, inaccurate, misleading, or not up to date Personal Data that Thai Union has been collecting, using and/or disclosing.

8. Procedures for Data Breach

In the event of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or accession to Personal Data, the relevant Employee and Data Administrator shall **immediately, but not later than 12 (twelve) hours**, notify the Management, the DPO and the email address provided in contact details below with the appropriate details of the breach.

9. Departmental Procedure

All relevant Departments/ Shared Service Units/ Business Units who related to the Personal Data shall issue and announce the Departmental Procedure. The Departmental Procedure shall consist of at least the following matters.

(1) Definition
(2) Responsible Person
(3) Collection of Personal Data
(4) Source of Personal Data
(5) Informing of the Collection Purpose and Right
(6) Data Protection Process including Internal Audit Measures
(7) Data Subject's Right
(8) Contact Person

(9) Data Flow and Security

Example of Departmental Procedure is in the below Appendix No.2.

10. Contact details

If you any question regarding this policy, please find contact detail below.

Email: PersonalData@ThaiUnion.com

Approved on 26 May 2022

-Signed by-	*-Signed by-*
(Mr.Thiraphong Chansiri)	(Mr. Shue Chung Chan)
President & CEO	Group Director, Corporate Office

Appendix No.1

Template of Privacy Notice

Privacy Notice for [Data Subject]

[Company's Name] ("Company") would like to provide information related to Company's policy on Personal Data protection concerning [Project's name] including but not limited to how the personal data of [Data Subject] will be collected, used and disclosed in accordance with provisions of the Personal Data Protection Act, EU General Data Protection Regulation and other applicable laws and regulations. This Notice provide important information in the following area:

1. **Objectives for Personal Data Collection**

   Company would like to inform about the objectives of collecting, using and disclosing your Personal Data as follows:

No.	Objectives of activities	Lawful basis
1.	[To/For .....] *Tell people the reasons why you need to collect or hold their information.	[Legal Obligation/Contractual Basis/Legitimate Interests/Consent] *Tell people Lawful basis for doing this in activities, please see explain in Note as below.

2. **Collected Data**

   For Objectives as specified above, Company is required to collect, use, process and disclose your Personal Data as follows:

   - Personal identifiers, contacts and characteristics (for example, name and contact details)
   - [Add to this list as appropriate]

   * Tell people about the type of personal information you collect. Personal information is any information that can be used to identify a living person. For example, members' email addresses, customer financial information, employee data or website user stats.

3. **Retention**

   Your personal information will be collected for as long as necessary to satisfy the purposes for which your personal data has been collected. Company will collect data related to your transaction and will keep such information as long as necessary to achieve the objective of that particular transaction.

4. **Disclosure of Personal Data**

   Company may be required to disclose your Personal Data internally and may need to disclose Personal Data to a third party, both within Thailand [and in other countries (if any)], who have appropriate personal data protection standards. In this regard, Company will provide appropriate contract to protect your Personal Data:

   - [List of third party]

   * Tell people about any instances in which you pass personal information to a third party and outline your reasons for this.

5. **Accessing website (if any)**

   Company is obliged under Thai law to retain your computer traffic data, for at least ……. (…....) days from the date you entered Company' s website. However, Company will not use such data to analyze consumption behavior or conduct market research without your explicit consent.

6. **Cookies (if any)**

   Cookies are small text files that are stored on your computer's browser or devices when you connect or visit any website to navigate you through our website, deliver user friendly and more personalized services to you. However, Cookies will not collect information stored on your computer ("Cookies").

Company uses Cookies to learn more about how you interact with the content on our website in order to give you more satisfaction when using our website. Cookies will remember the browser you used and installed while you are on our website. In addition, Cookies remember your preferences such as languages used and regions and automatically adjusts settings when you return to our website. Some of the Cookies are session Cookies and some are persistent Cookies which will be stored on your computer for a longer period.

For certain operations, Company will use third party services provider, for example, to track and analyse statistical use and information of users of the Company website in order to customize our website according to your individual interests and manage content on the website.

Company will not use Cookies to collect personal information. If you do not want to accept Cookies you may choose to decline Cookies or block Cookies sent by Company or third-party service providers by changing the settings in your browser (you can find more information in the Help menu of your browser). However, most browsers accept Cookies automatically. If you do not wish to accept cookies, you may have to constantly block or delete cookies.

7. Your Rights

As a Data Subject, you have the following rights:

- To withdraw consent for the collection, use or disclose Personal Data;
- To request access to and obtain a copy of your Personal Data or to request the disclosure of the acquisition of your Personal Data obtained without consent;
- To request to obtain Personal Data and request the transfer of Personal Data to a third party if it can be done automatically;
- To object to the collection, use or disclosure of the Personal Data;
- To request to erase or destroy Personal Data, or anonymise the Personal Data to become anonymous;
- To request to restrict the use of Personal Data;
- To request to update, complete and not misleading of Personal Data collected.

You can exercise your rights by sending Company an email or sending a written notice to Company, attaching a copy of your ID or equivalent details as requested. Company will process such information received in accordance with, and to the extent permitted, by applicable laws.

Please note that Company shall retain our rights under the laws to reject your request in certain circumstances. If Company decides to reject your request, you will be notified of the reason for such rejection. Company will try our best, also with considering technical capabilities, to answer your request on how we process your Personal Data. However, if you have unresolved concerns, you can complain to Company or proceed further to the Data Protection Authorities.

8. Protection of Personal Data

Company is committed to protecting your Personal Data under our security standards, and will provide appropriate safeguards to protect your Personal Data in order to ensure that Personal Data will be legally and appropriately collected, used or disclosed.

9. Changes to Privacy Notice

Company reserves the right to make changes to this Notice to be appropriate and in accordance with any laws. Please frequently check to see any updates or changes to Company's Privacy Notice.

10. Contact

If you have any enquiries or would like to exercise your rights or need any help regarding your personal data, please send an email to: [Email] and provide us with your personal information together with evidence to verify your identity such as ID card. However, Company may ask for additional relevant documents or may reject your request if Company has received insufficient information.

Note: Lawful Basis explanations (Personal Data Protection Act B.E.2562, section 24 and 26)

1. ***Consent*** means it is necessary for sensitive data and any purpose out of no.2 – no.7. For consent basis, the Data Subject must sign in a consent form.
2. ***Legal Obligation*** means it is necessary for compliance with a law to which the Data Controller is subjected.
3. ***Contractual Basis*** means it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.
4. ***Legitimate Interests*** means it is necessary for legitimate interests of the Data Controller or any other Persons or juristic persons other than the Data Controller, except where such interests are overridden by the fundamental rights of the data subject of his or her Personal Data.
5. ***Public Task*** means it is necessary for the performance of a task carried out in the public interest by the Data Controller, or it is necessary for the exercising of official authority vested in the Data Controller.
6. ***Vital Interest*** means it is for preventing or suppressing a danger to a Person's life, body or health.
7. ***Scientific / Historical Research*** means it is for the achievement of the purpose relating to the preparation of the historical documents or the archives for public interest, or for the purpose relating to research or statistics, in which the suitable measures to safeguard the data subject's rights and freedoms are put in place and in accordance with the notification as prescribed by the Committee.

Appendix No.2

Template and Example of Departmental Procedure

1. Template for Departmental Procedure (Blank Form)

Departmental Procedure on Personal Data Protection for Department Name

1. Definition

Data Subject means [Please fill in a person who collected, used, processed and disclosed their Personal Data (e.g. customer, visitor, supplier etc.)]

Personal Data means any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased persons in particular.

2. Responsible Person

[Head of Departments/ Shared Service Units/ Business Units] ("The Management") is a responsible person who oversee and ensure the classification of Personal Data collected, used or disclosed according to a purpose that notified to Customer including but not limit to provide a data security measure and audit measure to be ensure the Personal Data is updated, correct and accurate.

The Management shall appoint Data Administrator to be an assistant for monitoring and managing the Customer Personal Data.

3. Collection of Personal Data

Collection of Personal Data only is according to the purpose notified to Data Subject.

Thai Union does not collect Sensitive Personal Data that may cause discrimination or unfair bias to the Data Subjects without their explicit consent, except if it is collected under the PDPA.

Thai Union Collects Personal Data such as [type of Personal Data e.g. name, phone no.] for [purpose to collect Personal Data]

Collection of Personal Data has to be based on (1) contractual basis, for the initiation or fulfilment of a contract with Customers; (2) legal obligation, for the fulfilment of legal obligations; (3) legitimate interest, for the purpose of legitimate interests and the legitimate interests of third party. Thai Union will balance the legitimate interest pursued by Thai Union and Customers' interest, fundamental rights and freedoms in relation to the protection of Customers' Personal Data; (4) for preventing or suppressing a danger to a person's life, body or health; and/or (5) public interest, for the performance of a task carried out in the public interest or for the exercising of the state authorities (6) for establishment and raising of potential legal claims or other legal bases permitted under applicable laws relating to Personal Data protection (as the case may be). Depending on the context of the relationship with Thai Union, Thai Union may collect, use and/ or disclose Personal Data for the following purposes:

1) .....
2) .....
3) .....
4) .....
5) .....

4. Source of Personal Data

Receiving Personal Data directly from Data Subject via the following methods:

a) .....
b) .....

5. Informing of the Collection Purpose and Right

The Data Subject are informed of the purpose of collecting, using and disclosure their Personal Data, as well as their terms and rights and requested their consents (if any) prior to collection, processing or disclosure by .....

6. Data Protection Process including Internal Audit Measures

6.1 Purpose

Data Subject is collected and used only necessary to the informed purposes.

6.2 Storage

a) Hard Copy: .....

b) Soft Copy: .....

6.3 Collecting Process: limitation of collecting Customer's Personal Data as follows;

a) Collecting documents in hard copy and soft copy to verify identity such as name, surname, address, phone number, email, requirement during a preparing process until execution of an agreement.

b) Collecting documents in hard copy and soft copy to verify identity for processing products/services such as site visit (if any) before starting a project/transaction.

c) Collecting Customer's specification, additional requirement or amendment of scope of service (if any) on processing project/transaction.

6.4 When the retention period expires or Thai Union has no right or legitimate purpose for processing the Customer's Personal Data, Thai Union will proceed with the destruction and deletion of Personal Data where the Personal Data documents will be destroyed with a shredder and all electronic Personal Data will be deleted from the system.

6.5 Processing of Personal Data

Once receiving Personal Data, the Personal Data will be processed as follows:

❒ Collection: The relevant Employees will maintain the Personal Data in the specified file or folder and will maintain it in accordance with clause 6.6 [and if you internal transfer/share to other department, please specify]

❒ Use: The relevant Employees will use the Personal Data for the informed purposes.

❒ Disclosure to a third party such as [if you transfer/share to someone for processing, please specify] with the execution of the NDA and the DPA prior to the disclosure.

6.6 Retention Period

Data Administrator shall retain Data Subject's Personal Data for .... (....) year after the termination or expiration of the agreement, and delete/destroy the Personal Data within .... (....) days after such retention period.

6.7 Security

Data Administrator shall maintain appropriate security measures, which includes administrative, technical and physical safeguards in relation to access control, to protect the confidentiality, integrity, and availability of Personal Data against any accidental or unlawful or unauthorized loss, alteration, correction, use, disclosure or access, in compliance with the applicable laws.

In particular, implemented access control measures which are secured and suitable for the collection, use, and/or disclosure of Data Subject's Personal Data. And restrict access to Data Subject's Personal Data as well as storage and processing equipment by imposing access rights or permission, user, access management to limit access to Data Subject's Personal Data to only authorized persons, and implement user responsibilities to prevent unauthorized access, disclosure, perception, unlawful duplication of Data Subject's Personal Data or theft of device used to store and process Data Subject's Personal Data. This also includes measures that enables the re-examination of unauthorized access, alteration, erasure, or transfer of Data Subject's Personal Data which is suitable for the method and means of collecting, using and/or disclosing of Data Subject's Personal Data.

6.8 Audit Measures

Data Administrator shall monitor and control in order to ensure Personal Data updated and accurate including review Personal Data's collection, use, storage, retention period, security and breach from time to time.

If the Data Subject wish to update their Personal Data during the processing of the Personal Data. Thai Union will update the Data Subject's Personal Data to be accurate and up-to-date as notified.

6.9 Data Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, User and Data Administrator shall immediately, but not later than 12 hours, notify the manager-in-line and report to Thai Union via the email address provided in contact details below with the appropriate details of the incident.

7. Data Subject's Right

7.1 Right to Withdraw Consent: For the purposes the Data Subjects have consented to the collection, use and/or disclosure of Personal Data, Data Subjects may have the right to withdraw consent at any time.

7.2 Right to Access: Data Subjects may have the right to access or request a copy of the Personal Data which Thai Union has been collecting, using and/or disclosing. For privacy and security, Thai Union may require proof of the Data Subject's identity before providing the requested Personal Data.

7.3 Right to Data Portability: Data Subjects may have the right to obtain Personal Data in a structured, electronic format, and to transmit such Personal Data to another Data Controller, where (a) the Data Subjects have provided the Personal Data to Thai Union, and (b) if Thai Union has been collecting, using and/or disclosing that Personal Data on the basis of Data Subject's consent or other legitimate purposes.

7.4 Right to object: Data Subjects may have the right to object to certain collection, use and/or disclosure of Personal Data.

7.5 Right to Erasure: Data Subjects may have the right to request Thai Union to delete, destroy or anonymize Personal Data that Thai Union has been collecting, using, and/or disclosing, except that Thai Union is not obligated to do so if Thai Union needs to retain such Personal Data in order to comply with a legal obligation or to establish, exercise or defend legal claims.

7.6 Right to Rectification: Data Subjects may have the right to request for any rectification of incomplete, inaccurate, misleading, or not up to date Personal Data that Thai Union has been collecting, using and/or disclosing.

7.7 Right to Restriction: Data Subjects may have the right to restrict the use of Personal Data where the Data Subject believes such Personal Data is inaccurate, that the collection, use and/or disclosure is unlawful, or that Thai Union no longer needs such Personal Data for a particular purpose.

8. Contact Person

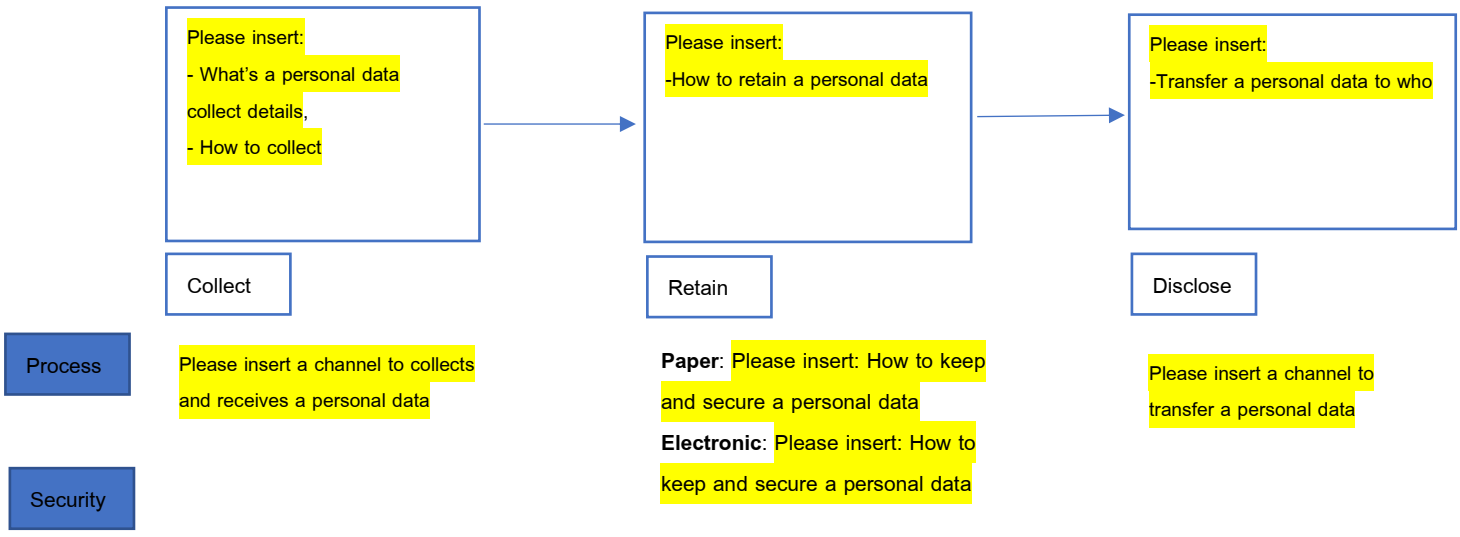
Responsible Person/Data Administrator

Name……..

Email……

Phone……

9. Data Flow and Security



2. Example of Departmental Procedure on Personal Data Protection for Marketing Department

1. Definition

Customers mean persons who purchase products and/or use services of Thai Union and/or those who are expected to purchase products and/or use the services of Thai Union (prospective Customers) including a person who are related to or are representatives of customers, such as executives, directors, employees, representatives, or personnel of customers who are juristic persons, including persons whose Personal Data appeared in relevant documents and processes, such as managers, purchasers, consignees, and cheque payers, etc.

Personal Data means any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased persons in particular.

2. Responsible Person

Department General Manager of Marketing (the Management) is a responsible person who oversee and ensure the classification of Personal Data collected, used or disclosed according to a purpose that notified to Customer including but not limit to provide a data security measure and audit measure to be ensure the Personal Data is updated, correct and accurate.

The Management shall appoint Data Administrator to be an assistant for monitoring and managing the Customer Personal Data.

3. Collection of Personal Data

Collection of Personal Data only is according to the purpose notified to Customer (Data Subject).

Thai Union does not collect Sensitive Personal Data that may cause discrimination or unfair bias to the Data Subjects without their explicit consent, except if it is collected under the PDPA.

Thai Union Collects Personal Data only necessary for verify identity and manage products/services such as name, surname, address, phone number, email, Customer requirement, invoice for the entry into agreements and other relevant processes, such as checking of evidence for the entry into agreements, consideration of credit limit, and providing collateral, etc.

Collection of Personal Data has to be based on (1) contractual basis, for the initiation or fulfilment of a contract with Customers; (2) legal obligation, for the fulfilment of legal obligations; (3) legitimate interest, for the purpose of legitimate interests and the legitimate interests of third party. Thai Union will balance the legitimate interest pursued by Thai Union and Customers' interest, fundamental rights and freedoms in relation to the protection of Customers' Personal Data; (4) for preventing or suppressing a danger to a person's life, body or health; and/or (5) public interest, for the performance of a task carried out in the public interest or for the exercising of the state authorities (6) for establishment and raising of potential legal claims or other legal bases permitted under applicable laws relating to Personal Data protection (as the case may be).

Depending on the context of the relationship with Thai Union, Thai Union may collect, use and/ or disclose Personal Data for the following purposes:

1) To operate Thai Union's business.
2) To register and verify.
3) To provide marketing communications.
4) To improve business operation, products and services.
5) To comply with legal obligations and orders from the government agencies.

4. Source of Personal Data

Receiving Personal Data directly from Customers via the following methods:

a) When Customers engage in communications or make enquiries, provide comments or feedbacks to Thai Union, regardless of whether in written or oral communications through the website, application, by phone, e-mail, fax, mail, by face-to-face interaction or by any other means; and/or

b) When Customers express an intention to purchase products or use services of Thai Union, enter into a contract with Thai Union, or deliver documents containing Personal Data to Thai Union.

5. Informing of the Collection Purpose and Right

The Customers are informed of the purpose of collecting, using and disclosure their Personal Data, as well as their terms and rights and requested their consents (if any) prior to collection, processing or disclosure by being sent together with agreement, quotation or proposal etc.

6. Data Protection Process including Internal Audit Measures

6.1 Purpose

Customer's Personal Data is collected and used only necessary to the informed purposes.

6.2 Storage

c) Hard Copy: Customer's documents such as copy of identification, copy of passport, copy of house register, requirement specification are stored in the secured customer list file.

d) Soft Copy: copy of Customer's documents such as pdf files are securely saved in folder name customer list.

6.3 Collecting Process: limitation of collecting Customer's Personal Data as follows;

d) Collecting documents in hard copy and soft copy to verify identity such as name, surname, address, phone number, email, requirement during a preparing process until execution of an agreement.

e) Collecting documents in hard copy and soft copy to verify identity for processing products/services such as site visit (if any) before starting a project/transaction.

f) Collecting Customer's specification, additional requirement or amendment of scope of service (if any) on processing project/transaction.

6.4 When the retention period expires or Thai Union has no right or legitimate purpose for processing the Customer's Personal Data, Thai Union will proceed with the destruction and deletion of Personal Data where the Personal Data documents will be destroyed with a shredder and all electronic Personal Data will be deleted from the system.

6.5 Processing of Personal Data

Once receiving Personal Data, the Personal Data will be processed as follows:

❒ Collection: The relevant Employees will maintain the Personal Data in the specified file or folder and will maintain it in accordance with clause 6.6 and send it to the accounting department for receipt of payment.

❒ Use: The relevant Employees will use the Personal Data for the informed purposes.

❒ Disclosure to a third party such as service providers, airlines, accommodation, etc. with the execution of the NDA and the DPA prior to the disclosure.

6.6 Retention Period

Data Administrator shall retain Customer's Personal Data for 1 (one) year after the termination or expiration of the agreement, and delete/destroy the Personal Data within 30 (thirty) days after such retention period.

6.7 Security

Data Administrator shall maintain appropriate security measures, which includes administrative, technical and physical safeguards in relation to access control, to protect the confidentiality, integrity, and availability of Personal Data against any accidental or unlawful or unauthorized loss, alteration, correction, use, disclosure or access, in compliance with the applicable laws.

In particular, implemented access control measures which are secured and suitable for the collection, use, and/or disclosure of Customer's Personal Data. And restrict access to Customer's Personal Data as well as storage and processing equipment by imposing access rights or permission, user, access management to limit access to Customer's Personal Data to only authorized persons, and implement user responsibilities to prevent unauthorized access, disclosure, perception, unlawful duplication of Customer's Personal Data or theft of device used to store and process Customer's Personal Data. This also includes measures that enables the re-examination of unauthorized access, alteration, erasure, or transfer of Customer's Personal Data which is suitable for the method and means of collecting, using and/or disclosing of Customer's Personal Data.

6.8 Audit Measures

Data Administrator shall monitor and control in order to ensure Personal Data updated and accurate including review Personal Data's collection, use, storage, retention period, security and breach from time to time.

If the Customers wish to update their Personal Data during the processing of the Personal Data. Thai Union will update the Customer's Personal Data to be accurate and up-to-date as notified.

6.9 Data Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, User and Data Administrator shall immediately, but not later than 12 hours, notify the manager-in-line and report to Thai Union via the email address provided in contact details below with the appropriate details of the incident.

7. Data Subject's Right

7.1 Right to Withdraw Consent: For the purposes the Data Subjects have consented to the collection, use and/or disclosure of Personal Data, Data Subjects may have the right to withdraw consent at any time.

7.2 Right to Access: Data Subjects may have the right to access or request a copy of the Personal Data which Thai Union has been collecting, using and/or disclosing. For privacy and security, Thai Union may require proof of the Data Subject's identity before providing the requested Personal Data.

7.3 Right to Data Portability: Data Subjects may have the right to obtain Personal Data in a structured, electronic format, and to transmit such Personal Data to another Data Controller, where (a) the Data Subjects have provided the Personal Data to Thai Union, and (b) if Thai Union has been collecting, using and/or disclosing that Personal Data on the basis of Data Subject's consent or other legitimate purposes.

7.4 Right to object: Data Subjects may have the right to object to certain collection, use and/or disclosure of Personal Data.

7.5 Right to Erasure: Data Subjects may have the right to request Thai Union to delete, destroy or anonymize Personal Data that Thai Union has been collecting, using, and/or disclosing, except that Thai Union is not obligated to do so if Thai Union needs to retain such Personal Data in order to comply with a legal obligation or to establish, exercise or defend legal claims.

7.6 Right to Rectification: Data Subjects may have the right to request for any rectification of incomplete, inaccurate, misleading, or not up to date Personal Data that Thai Union has been collecting, using and/or disclosing.

7.7 Right to Restriction: Data Subjects may have the right to restrict the use of Personal Data where the Data Subject believes such Personal Data is inaccurate, that the collection, use and/or disclosure is unlawful, or that Thai Union no longer needs such Personal Data for a particular purpose.

8. Contact Person

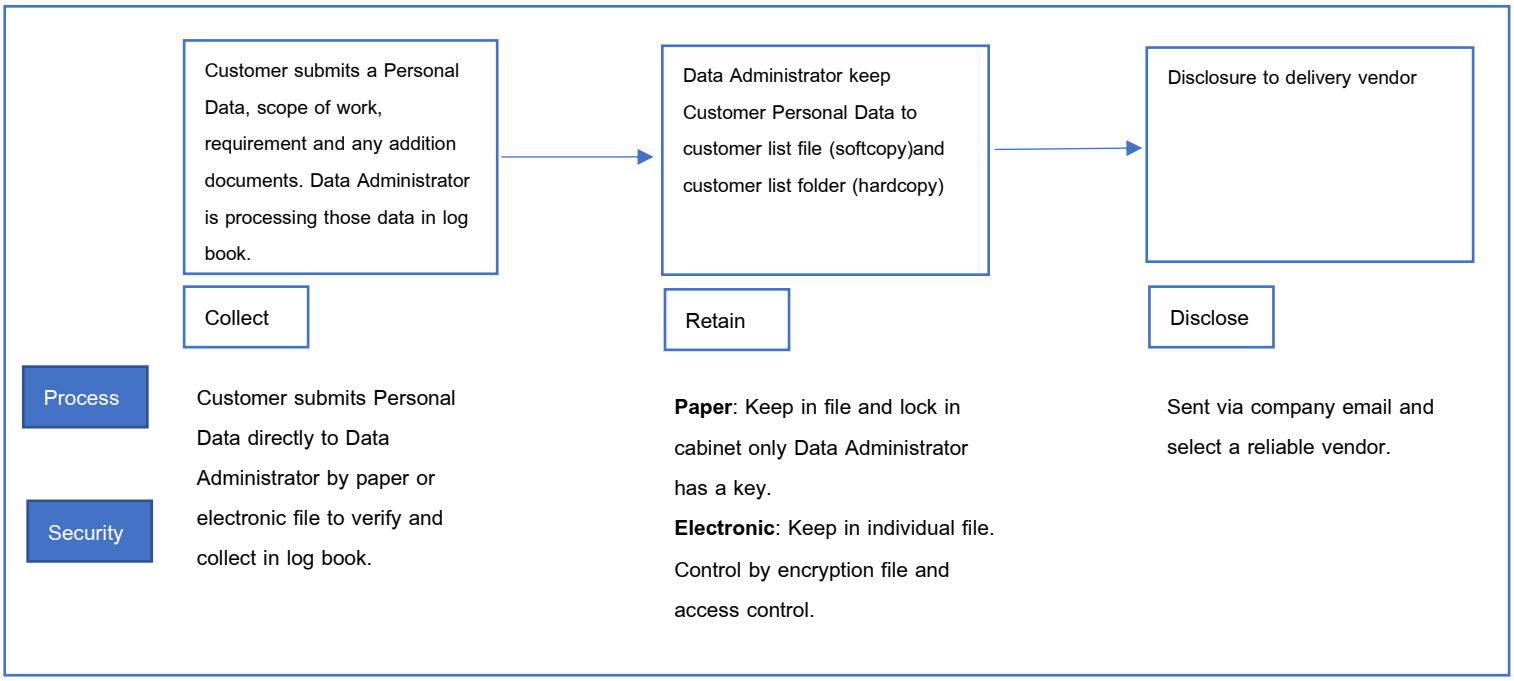
Responsible Person/Data Administrator

Name: Abc Def

Email: Abc.Def@thaiunion.com

Phone: 02-298-0024

9. Data Flow and Security



คำแปล

สารบัญ

นโยบายคุ้มครองข้อมูลส่วนบุคคล

1. คำนำ

เนื่องจากในหลายประเทศได้เริ่มพัฒนาและออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลของตนเอง ภายหลังจากการบังคับใช้กฎระเบียบให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค (GDPR) ในปี พ.ศ. 2561 กฎหมายว่าด้วยการคุ้มครองข้อมูลจึงถือเป็นเรื่องปกติในทุกประเทศทั่วโลก

บริษัท ไทยยูเนี่ยน กรุ๊ป จำกัด (มหาชน) เป็นบริษัทชั้นนำด้านอาหารทะเลระดับโลกที่เน้นความยั่งยืนและมุ่งสร้างความพึงพอใจให้กับลูกค้าด้วยผลิตภัณฑ์ที่มีคุณภาพ และเพื่อเป็นการปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับการคุ้มครองข้อมูล (รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย (“**PDPA**”)) และเพื่อปกป้องข้อมูลส่วนบุคคลของผู้มีส่วนได้ส่วนเสียของเรา ซึ่งรวมถึงลูกค้าและพนักงานของเราจากการใช้โดยมิได้รับอนุญาตและการสูญเสียที่ผิดกฎหมาย เราจึงกำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล (“**นโยบาย**”) เพื่อดำเนินการตามระเบียบปฏิบัติที่เหมาะสมสำหรับการรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล

นโยบายนี้จะครอบคลุมถึงข้อมูลของบุคคลที่ถูกรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของพวกเขาด้วย

2. วัตถุประสงค์

นโยบายนี้ได้กำหนดข้อบังคับสำหรับบริษัท ไทยยูเนี่ยน กรุ๊ป จำกัด (มหาชน) บริษัทลูกและบริษัทในเครือทั้งหมดในประเทศไทย (โดยเรียกรวมกันหรือแยกกันว่า “**ไทยยูเนี่ยน**”) เพื่อให้เป็นที่แน่ใจว่าข้อมูลส่วนบุคคลทั้งหมดจะได้รับการปฏิบัติดังต่อไปนี้

ก. ดำเนินการต่อเจ้าของข้อมูลอย่างถูกต้องตามกฎหมายและด้วยความโปร่งใส
ข. เก็บรวบรวมเพื่อวัตถุประสงค์อันเป็นการเฉพาะ ชัดแจ้ง และชอบด้วยกฎหมายอื่นๆ และไม่ดำเนินการในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว
ค. เก็บข้อมูลเท่าที่จำเป็นและเพียงพอเพื่อใช้สำหรับการประมวลผลตามวัตถุประสงค์
ง. ทำให้ถูกต้องและปรับปรุงให้เป็นปัจจุบันเมื่อจำเป็น โดยต้องดำเนินการตามสมควรทุกขั้นตอนเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่คลาดเคลื่อนที่ได้รับการประมวลผลตามวัตถุประสงค์นั้น ได้ถูกลบหรือแก้ไขโดยไม่ล่าช้า และ
จ. ได้รับการประมวลผลในลักษณะที่เป็นการรับรองความปลอดภัยที่เหมาะสมต่อข้อมูลส่วนบุคคล รวมถึงการป้องกันการประมวลผลโดยไม่ได้รับอนุญาตหรือที่ผิดกฎหมาย และต่อการสูญเสีย การทำลาย หรือความเสียหายโดยไม่ได้ตั้งใจ โดยใช้มาตรการทางเทคนิคหรือมาตรการขององค์กรที่เหมาะสม

ประธานเจ้าหน้าที่บริหาร กรรมการผู้จัดการ ผู้บริหาร และพนักงานทุกคน ต้องรักษาความลับ ความสมบูรณ์ และการมีอยู่ของข้อมูลส่วนบุคคลทั้งหมด เพื่อการปฏิบัติตาม PDPA

นโยบายนี้และเอกสารที่เกี่ยวข้องจะได้รับการตรวจสอบเป็นครั้งคราว หรือเมื่อใดก็ตามที่กฎหมายที่สามารถบังคับใช้หรือสภาพแวดล้อมทางธุรกิจของไทยยูเนี่ยนได้เปลี่ยนแปลงไปในลักษณะที่ส่งผลต่อนโยบายในปัจจุบัน

3. คำจำกัดความ

ตามวัตถุประสงค์ของนโยบายนี้ ข้อกำหนดที่กำหนดไว้ด้านล่างให้มีความหมายตามที่ระบุไว้ดังต่อไปนี้
คณะกรรมการบริษัท หมายถึง กรรมการของไทยยูเนี่ยน
ประธานเจ้าหน้าที่บริหารหรือกรรมการผู้จัดการ หมายถึง ประธานเจ้าหน้าที่บริหาร กรรมการผู้จัดการ หรือตำแหน่งฝ่ายบริหารระดับสูงของไทยยูเนี่ยน
คุกกี้ หมายถึง ไฟล์ข้อความขนาดเล็กที่ถูกสร้างขึ้นโดยเว็บไซต์และจะถูกเก็บไว้ในคอมพิวเตอร์หรืออุปกรณ์สื่อสารของผู้ใช้งาน ซึ่งจะเก็บรวบรวมข้อมูลส่วนบุคคล การใช้งาน และการตั้งค่าอื่นๆของผู้ใช้งานเพื่อปรับปรุงประสบการณ์ของผู้ใช้เว็บไซต์
ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนก หมายถึง ผู้ที่ได้รับการแต่งตั้งจากผู้บริหารของแต่ละแผนก/ หน่วยบริการร่วม/ หน่วยธุรกิจ ให้ดูแลและตรวจสอบกระบวนการที่เกี่ยวข้องทั้งหมด รวมทั้งมีอำนาจในการจัดจำแนกประเภท ดูแลและตรวจสอบข้อมูลส่วนบุคคลเพื่อให้สอดคล้องกับนโยบายนี้และนโยบายที่เกี่ยวข้อง ตามระเบียบปฏิบัติและระเบียบปฏิบัติของแผนก เช่น รูปแบบการจัดประเภทข้อมูล

ของไทยยูเนี่ยน ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกยังมีอำนาจในการกำหนดและเพิกถอนสิทธิของพนักงานในการเข้าถึงข้อมูลส่วนบุคคลด้วย

ผู้ควบคุมข้อมูล หมายถึง บุคคลที่พิจารณาตัดสินใจในการรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลใด ๆ ของเจ้าของข้อมูล

ผู้ประมวลผลข้อมูล หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงานสาธารณะ หน่วยงาน หรือกลุ่มบุคคลอื่นใด ที่ดำเนินการรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในนามของหรือภายใต้ชื่อของผู้ควบคุมข้อมูล ซึ่งผู้ประมวลผลข้อมูลให้รวมถึงผู้ประมวลผลย่อยทั้งหมด

การประเมินผลกระทบในการคุ้มครองข้อมูล (**DPIA**) หมายถึง กระบวนการที่ออกแบบมาเพื่ออธิบายการประมวลผล ประเมินความจำเป็นและความได้สัดส่วน และดูแลความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล อันเป็นผลมาจากการประมวลผลข้อมูลส่วนบุคคล โดยการประเมินและการกำหนดมาตรการเพื่อใช้ควบคุม

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (**DPO**) หมายถึง บุคคลหรือกลุ่มบุคคลที่ได้รับการแต่งตั้งภายใต้นโยบายนี้ให้ปฏิบัติหน้าที่ของ DPO ตามที่ PDPA หรือระเบียบอื่นใดที่เกี่ยวข้องกำหนด และมีหน้าที่รับผิดชอบในการให้คำปรึกษาและตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลเพื่อให้สอดคล้องกับ PDPA

เจ้าของข้อมูล หมายถึง บุคคลธรรมดาที่สามารถระบุตัวตนได้โดยข้อมูลส่วนบุคคล

ระเบียบปฏิบัติของแผนก หมายถึง ระเบียบปฏิบัติของแผนกที่ออกและประกาศโดยแผนก/ หน่วยบริการร่วม/ หน่วยธุรกิจที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

DPA หมายถึง สัญญาประมวลผลข้อมูลส่วนบุคคล

DSA หมายถึง สัญญาแลกเปลี่ยนข้อมูลส่วนบุคคล

พนักงาน หมายถึง พนักงานทุกคนของไทยยูเนี่ยน

ผู้บริหาร หมายถึง ผู้บริหารแผนก /หน่วยบริการร่วม/ หน่วยธุรกิจ ที่อยู่ภายใต้ไทยยูเนี่ยน

NDA หมายถึง สัญญาไม่เปิดเผยข้อมูล

สำนักงาน หมายถึง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPA หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย รวมถึงระเบียบ ประกาศ และข้อกำหนดต่างๆ

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลส่วนบุคคลใด ๆ ที่สามารถระบุตัวบุคคลได้ไม่ว่าโดยตรงหรือโดยอ้อม แต่ไม่รวมถึงข้อมูลของผู้เสียชีวิต

นโยบาย หมายถึง นโยบายคุ้มครองข้อมูลส่วนบุคคลนี้

ประกาศความเป็นส่วนตัว หมายถึง คำประกาศเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่แจ้งให้เจ้าของข้อมูลทราบ

ระเบียบปฏิบัติ หมายถึง ระเบียบปฏิบัติใด ๆ ที่ออกมาเพื่อชี้แจงรายละเอียดการดำเนินงานสำหรับการปฏิบัติตามนโยบายนี้

ข้อมูลส่วนบุคคลที่ละเอียดอ่อน หมายถึง ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและห้ามมิให้รวบรวมโดยไม่ได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล ซึ่งรวมถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสัญชาติ เชื้อสาย สีผิว ความคิดเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลด้านสุขภาพ ความทุพพลภาพ ข้อมูลสหภาพแรงงาน ข้อมูลทางพันธุกรรม ข้อมูลทางชีววิทยา และข้อมูลส่วนบุคคลอื่น ๆ ตามที่ PDPA กำหนด

ผู้ประมวลผลย่อย หมายถึง บุคคลภายนอกที่ติดต่อโดยผู้ประมวลผลเพื่อให้ดำเนินการประมวลผลในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลในนามของผู้ประมวลผลข้อมูล

ไทยยูเนี่ยน หมายถึง บริษัท ไทยยูเนี่ยน กรุ๊ป จำกัด (มหาชน) บริษัทลูกและบริษัทในเครือทั้งหมดในประเทศไทย

บุคคลภายนอก หมายถึง บุคคลธรรมดาหรือนิติบุคคลนอกเหนือไปจากเจ้าของข้อมูลหรือผู้ควบคุมข้อมูลซึ่งเป็นผู้รับหรือผู้ประมวลผลข้อมูลส่วนบุคคล

4. หน้าที่และความรับผิดชอบ

4.1 คณะกรรมการของบริษัท

4.1.1 พิจารณาและอนุมัตินโยบาย

4.1.2 ควบคุมและกำกับดูแลให้แน่ใจว่านโยบายและระเบียบปฏิบัติที่เกี่ยวข้องได้รับการปฏิบัติตามและนำไปใช้อย่างสมบูรณ์ในไทยยูเนี่ยน

4.2 ประธานเจ้าหน้าที่บริหารหรือกรรมการผู้จัดการ

4.2.1 แต่งตั้ง DPO ให้กับแต่ละหน่วยงานเพื่อปฏิบัติหน้าที่ของ DPO ตาม PDPA และตามนโยบายนี้

4.2.2 ติดตามตรวจสอบและกำกับดูแลว่านโยบายและระเบียบปฏิบัติที่เกี่ยวข้องได้รับการปฏิบัติตามและนำไปใช้อย่างสมบูรณ์ในหน่วยงานที่เกี่ยวข้องภายใต้ไทยยูเนี่ยน

4.3 ผู้บริหาร

4.3.1 กำกับดูแลให้แน่ใจว่าแผนก / หน่วยบริการร่วม / หน่วยธุรกิจที่เกี่ยวข้อง ปฏิบัติตาม PDPA และตามนโยบายนี้ และผู้บริหารของแผนก / หน่วยบริการร่วม / หน่วยธุรกิจ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ

ก) ลูกค้า รวมถึงกรรมการบริษัทของลูกค้า ตัวแทน ผู้มีอำนาจ หรือบุคคลอื่นที่ทำงานในนามของลูกค้า

ข) คู่ค้าทางธุรกิจ รวมถึงกรรมการบริษัท ตัวแทน ตัวแทนที่ได้รับมอบอำนาจ หรือบุคคลอื่นที่ทำงานในนามของคู่ค้าทางธุรกิจ

ค) ผู้สมัครงาน ผู้สมัครฝึกงาน และผู้ฝึกงาน

ง) พนักงาน ผู้เข้ารับการฝึกอบรม และสมาชิกในครอบครัว

จ) ผู้ถือหุ้นและกรรมการบริษัท

ฉ) ผู้เข้าเยี่ยมชมและผู้เข้าร่วมกิจกรรม และ/หรือ

ช) บุคคลอื่นใดซึ่งแผนก/ หน่วยบริการร่วม/ หน่วยธุรกิจ ได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของพวกเขา

จะต้องจัดทำและประกาศระเบียบปฏิบัติของแผนกโดยละเอียด (ตามที่อธิบายไว้ในข้อ 9) สำหรับการปฏิบัติงานประจำวัน

4.3.2 แต่งตั้งให้มีผู้รับผิดชอบเพื่อปฏิบัติหน้าที่เป็นผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนก (ตามที่อธิบายไว้ในข้อ 4.6) ของนโยบายนี้

4.3.3 กำกับดูแลให้แน่ใจว่าเจ้าของข้อมูลได้รับแจ้งและรับทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงสิทธิของเจ้าของข้อมูล เช่น การแบ่งปันประกาศความเป็นส่วนตัวที่เกี่ยวข้องก่อนหรือขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โปรดดูแบบฟอร์มประกาศความเป็นส่วนตัวในภาคผนวกที่ 1

4.3.4 กำกับดูแลให้แน่ใจว่าการรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลนั้นสอดคล้องกับวัตถุประสงค์ตามที่ได้แจ้งต่อเจ้าของข้อมูลหรือตามที่ได้รับความยินยอม ในกรณีที่จำเป็นต้องได้รับความยินยอม ผู้บริหารจำเป็นต้องตรวจสอบให้แน่ใจว่าเจ้าของข้อมูลให้ความยินยอมตามนโยบาย ระเบียบปฏิบัติ และระเบียบปฏิบัติของแผนก

4.3.5 แจ้งแก่ DPO ทันทีในกรณีที่มีการละเมิดข้อมูล และปฏิบัติงานอย่างใกล้ชิดกับ DPO

4.3.6 ให้คำแนะนำแก่ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนก เพื่อดำเนินการตามคำขอสำหรับการใช้สิทธิของเจ้าของข้อมูล เช่น การแก้ไข ลบทิ้ง ทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้ตามคำขอของเจ้าของข้อมูล และเพื่อบันทึกและเก็บรักษาบันทึกการดำเนินการดังกล่าว

4.3.7 แต่งตั้งผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกอย่างน้อยหนึ่งคน เพื่อดูแลและตรวจสอบข้อมูลส่วนบุคคลที่ได้เก็บรวบรวม ใช้ และประมวลผลโดยแผนก/ หน่วยบริการร่วม/ หน่วยธุรกิจดังกล่าว

4.3.8 ดูแล ตรวจสอบ และทำให้แน่ใจว่าผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกได้ปฏิบัติหน้าที่ตามนโยบาย ระเบียบปฏิบัติและระเบียบปฏิบัติของแผนกดังกล่าวนี้

4.3.9 จัดกิจกรรมเสริมสร้างความตระหนักรู้และการอบรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

4.4 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

4.4.1 ให้คำแนะนำแก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล และพนักงานของผู้ควบคุมข้อมูลหรือของผู้ประมวลผลข้อมูลตามที่ PDPA และนโยบายนี้กำหนด

4.4.2 ตรวจสอบการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล และพนักงานของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล และพนักงานของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล ซึ่งเกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลตาม PDPA และนโยบายนี้กำหนด

4.4.3 ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีเหตุการณ์ใด ๆ อันเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล รวมทั้งพนักงานของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล รวมถึงบุคคลภายนอกด้วย

4.4.4 รักษาความลับของข้อมูลส่วนบุคคลที่ได้ทราบหรือได้มาเนื่องจากการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ภายใต้ PDPA และนโยบายนี้

ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลจะต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการปฏิบัติหน้าที่ โดยจัดหาเครื่องมือหรืออุปกรณ์และอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อปฏิบัติงานตามหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจมีการปฏิบัติหน้าที่อื่นๆ ซึ่งผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลจะต้องให้การรับรองแก่สำนักงานว่าการปฏิบัติหน้าที่ดังกล่าวนั้นไม่ฝ่าฝืนหรือขัดแย้งกับการปฏิบัติหน้าที่ภายใต้ PDPA

4.5 พนักงาน

4.5.1 กำกับดูแลและรับผิดชอบว่ากระบวนการเก็บรวบรวม การใช้ และการเปิดเผย (รวมถึงกระบวนการสำหรับการจัดจำแนกประเภทข้อมูล การประมวลผลข้อมูล การจัดเก็บข้อมูล การส่งข้อมูล การกำจัดข้อมูล และการทำลายข้อมูล) ของข้อมูลส่วนบุคคลนั้นสอดคล้องกับ PDPA นโยบายนี้ ระเบียบปฏิบัติและระเบียบปฏิบัติของแผนก

4.5.2 แจ้งเจ้าหน้าที่ DPO ทันทีเมื่อมีการละเมิดข้อมูลส่วนบุคคลหรือกรณีอื่นใด

4.5.3 แจ้งเจ้าหน้าที่ DPO และประธานเจ้าหน้าที่บริหารหรือกรรมการผู้จัดการ หรือรายงานผ่านช่องทางการรายงานของไทยยูเนี่ยนทันที หากมีการกระทำใด ๆ ที่อาจละเมิดต่อ PDPA หรือนโยบายนี้

4.6 ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนก

4.6.1 กำกับดูแลการเก็บรวบรวม การใช้ การเปิดเผย และการประมวลผลข้อมูลส่วนบุคคลของพนักงานในแผนก/ หน่วยบริการร่วม/ หน่วยธุรกิจ ให้เป็นไปตามที่ PDPA นโยบาย ระเบียบปฏิบัติและระเบียบปฏิบัติของแผนกกำหนด

4.6.2 บันทึกรายชื่อของพนักงานที่สามารถเข้าถึงข้อมูลส่วนบุคคลและการใช้ข้อมูลส่วนบุคคลของพนักงาน

4.6.3 บันทึกรายชื่อของผู้ประมวลผลข้อมูลและบุคคลภายนอกอื่นใดที่ได้รับข้อมูลส่วนบุคคลจากไทยยูเนี่ยน

4.6.4 ตรวจสอบให้แน่ใจว่าสัญญาไม่เปิดเผยข้อมูล (“NDA”) และสัญญาประมวลผลข้อมูล (“DPA”) ได้รับการลงนามอย่างสมบูรณ์ตามข้อ 5.7

4.6.5 ดำเนินการตามคำขอที่ร้องขอโดยเจ้าของข้อมูล เพื่อจัดการข้อมูลส่วนบุคคลตามที่ PDPA นโยบายนี้ ระเบียบปฏิบัติและระเบียบปฏิบัติของแผนกกำหนด

4.6.6 ตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลได้รับการจำแนกประเภทตามรูปแบบของการจัดประเภทข้อมูลของไทยยูเนี่ยน

5. การคุ้มครองข้อมูลส่วนบุคคล

5.1 การจำแนกประเภทข้อมูล

ข้อมูลส่วนบุคคลจะถูกจำแนกประเภทตามรูปแบบของการจัดประเภทข้อมูลของไทยยูเนี่ยน ซึ่งได้กำหนดไว้ในนโยบายการรักษาความปลอดภัยของข้อมูลของไทยยูเนี่ยน และข้อมูลส่วนบุคคลที่ระบุตัวบุคคลนั้นได้ (“PII”) - เอกสารอ้างอิงโดยคำนึงถึงมูลค่า ข้อกำหนดของกฎหมาย ความอ่อนไหวและความสำคัญของข้อมูลของไทยยูเนี่ยน ซึ่งแนวทางของไทยยูเนี่ยนในการจำแนกประเภทข้อมูลส่วนบุคคลจะกำหนดเพิ่มเติมโดยแผนก IT โดยข้อมูลส่วนบุคคลจะถูกประมวลผล จัดเก็บ ส่ง กำจัด และทำลายอย่างปลอดภัย โดยพนักงานที่ได้รับมอบหมายตามระดับการจำแนกประเภทข้อมูล และจะได้รับการดำเนินการตามรูปแบบของการจัดประเภทข้อมูลของไทยยูเนี่ยน

พนักงานมีหน้าที่รับผิดชอบในการกำหนดระดับการจำแนกประเภท โดยให้ข้อมูลที่อยู่ภายใต้ความรับผิดชอบของพนักงานเป็นไปตามรูปแบบของการจัดประเภทข้อมูลของไทยยูเนี่ยน และเพื่อให้มั่นใจว่าผู้รับข้อมูลตระหนักถึงระดับการจัดจำแนกประเภท ด้วยวิธีการแจ้งต่างๆ เช่น การติด แสดงป้าย หรืออีเมล เป็นต้น

5.2 การเก็บรวบรวมข้อมูล

5.2.1 การเก็บรวบรวมจะถูกจำกัดตามความจำเป็นเท่าที่เกี่ยวข้องกับวัตถุประสงค์ตามที่ไทยยูเนี่ยนกำหนด ภายใต้ความยินยอมของเจ้าของข้อมูล หรือตามหลักเกณฑ์ที่กำหนดใน PDPA ตัวอย่างเช่น (1) สำหรับการทำสัญญาหรือการร้องขอโดยเจ้าของข้อมูล (2) สำหรับพันธกรณีทางกฎหมาย (3) สำหรับผลประโยชน์ที่ชอบด้วยกฎหมาย (4) เพื่อผลประโยชน์ทางสาธารณะและ/หรือ (5) เพื่อป้องกันภยันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

5.2.2 เจ้าของข้อมูลจะได้รับแจ้งรายละเอียดดังต่อไปนี้

ก. วัตถุประสงค์ของการเก็บรวบรวม

ข. แจ้งถึงเหตุที่เจ้าของข้อมูลจำเป็นต้องให้ข้อมูล

ค. ระยะเวลาของการเก็บรวบรวม

ง. ประเภทของบุคคลหรือองค์กรที่อาจเปิดเผยข้อมูลส่วนบุคคล

จ. ข้อมูล ที่อยู่ และรายละเอียดการติดต่อของผู้ควบคุมข้อมูล

ฉ. สิทธิของเจ้าของข้อมูล

ช. ช่องทางสำหรับเจ้าของข้อมูลในการเพิกถอนความยินยอม

5.3 การใช้ข้อมูล

5.3.1 การใช้และการประมวลผลข้อมูลส่วนบุคคลจะเป็นไปตาม PDPA นโยบาย ระเบียบปฏิบัติและระเบียบปฏิบัติของแผนก นอกจากนี้ การใช้และการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจะต้องดำเนินการด้วยความปลอดภัยเป็นพิเศษ

5.3.2 เมื่อมีการประมวลผลข้อมูลส่วนบุคคล พนักงานจะต้องบันทึกรายละเอียดดังต่อไปนี้เพื่อให้เจ้าของข้อมูลสามารถตรวจสอบได้

ก. ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้

ข. วัตถุประสงค์ของการประมวลผลและการใช้ตามประเภทของข้อมูลส่วนบุคคล

ค. รายละเอียดของผู้ควบคุมข้อมูลส่วนบุคคล

ง. ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

จ. สิทธิและวิธีการในการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลดังกล่าว

ฉ. การใช้หรือการประมวลผลข้อมูลส่วนบุคคล และ

ช. การปฏิเสธการดำเนินการตามคำขอของเจ้าของข้อมูล

5.4 การเปิดเผยข้อมูล

5.4.1 พนักงานและบุคคลภายนอกจะต้องไม่เปิดเผยข้อมูลส่วนบุคคลใด ๆ นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งหรือได้รับความยินยอมของเจ้าของข้อมูล เว้นแต่ที่ได้กำหนดหรืออนุญาตโดย PDPA

5.5 การเก็บรักษาข้อมูล

ข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอิเล็กทรอนิกส์จะต้องถูกจัดเก็บอย่างปลอดภัยตามที่กำหนดไว้ใน PDPA และรูปแบบของการจัดประเภทข้อมูลของไทยยูเนี่ยนบนระบบคลาวด์ แอพพลิเคชั่น หรือระบบรักษาความปลอดภัยอื่น ๆ ที่อนุมัติโดยแผนก IT

นอกจากนี้ ข้อมูลส่วนบุคคลที่ไม่ได้อยู่ในรูปแบบอิเล็กทรอนิกส์จะต้องถูกเก็บไว้ในที่ปลอดภัย และการเข้าถึงที่จัดเก็บดังกล่าวจะถูกจำกัดด้วยการรักษาความปลอดภัยที่เหมาะสมตามระเบียบปฏิบัติ เพื่อหลีกเลี่ยงการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

เมื่อได้รับการให้ความยินยอมจากเจ้าของข้อมูล พนักงานจะต้องจัดเก็บการให้ความยินยอมดังกล่าวร่วมกับข้อมูลส่วนบุคคลในระบบและ/หรือที่จัดเก็บแห่งเดียวกัน

5.6 การโอนย้ายข้อมูล

ข้อมูลส่วนบุคคลอาจถูกโอนระหว่างพนักงานภายในไทยยูเนี่ยนได้เท่าที่จำเป็นสำหรับการปฏิบัติงาน และจำกัดการใช้เพื่อวัตถุประสงค์ทางธุรกิจที่ได้แจ้งตามที่กำหนดไว้ใน PDPA นโยบาย ระเบียบปฏิบัติและระเบียบปฏิบัติของแผนก

5.7 ผู้ประมวลผลข้อมูล / บุคคลภายนอก

5.7.1 หากพนักงานคนใดจำเป็นต้องโอนข้อมูลส่วนบุคคลไปยังผู้ประมวลผลข้อมูลใด ๆ นอกไทยยูเนี่ยน หรือข้อมูลส่วนบุคคลจะต้องถูกเก็บรวบรวม ใช้ และ/หรือประมวลผลโดยผู้ประมวลผลข้อมูลหรือถูกทำลายข้อมูลโดยบุคคลใด พนักงานจะต้องจัดให้ผู้ประมวลผลข้อมูลลงนามใน NDA และ DPA โดยใช้แบบฟอร์มของไทยยูเนี่ยน หรือ NDA และ DPA ซึ่งได้รับการอนุมัติโดยแผนกกฎหมายแล้ว และจะต้องตรวจสอบให้แน่ใจว่าผู้ประมวลผลข้อมูลมีมาตรฐานและมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เพียงพอ

หาก PDPA กำหนดให้ต้องแต่งตั้งตัวแทนผู้ประมวลผลข้อมูลในประเทศไทย พนักงานที่เกี่ยวข้องและผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องกำกับดูแลผู้ประมวลผลข้อมูลว่าได้ปฏิบัติตาม PDPA แล้ว ก่อนมีการจ้างผู้ประมวลผลข้อมูล นอกจากนี้ยังให้ใช้กับกรณีที่ผู้ประมวลผลข้อมูลเป็นบุคคลที่มีส่วนเกี่ยวข้องด้วย

ในกรณีที่ NDA และ DPA แตกต่างไปจากมาตรฐานของไทยยูเนี่ยน การร้องขอจะต้องทำเป็นลายลักษณ์อักษรโดยพนักงานที่เกี่ยวข้อง ซึ่งจะได้รับการตรวจสอบและอนุมัติโดยผู้บริหารและแผนกกฎหมายที่เกี่ยวข้อง ซึ่งการอนุมัติทั้งหมดในเรื่องนี้จะเป็นไปตามระดับความเสี่ยงที่อาจเกิดขึ้นและมาตรฐานความปลอดภัยของผู้ประมวลผลข้อมูล

5.7.2 หากพนักงานคนใดจำเป็นต้องแบ่งปันข้อมูลส่วนบุคคลกับบุคคลภายนอก พนักงานจะต้องจัดให้บุคคลภายนอกลงนามใน DSA โดยใช้แบบฟอร์มของไทยยูเนี่ยน หรือ DSA ที่ได้รับการอนุมัติโดยแผนกกฎหมายแล้ว และจะต้องตรวจสอบให้แน่ใจว่าผู้ประมวลผลข้อมูลมีความปลอดภัยและมาตรฐานการปกป้องข้อมูลที่เพียงพอ

5.8 การปรับปรุงข้อมูลให้เป็นปัจจุบันและถูกต้อง

พนักงานและผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องดำเนินการตามระเบียบปฏิบัติที่เหมาะสม เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นถูกต้องและเป็นปัจจุบันตามคำร้องขอของเจ้าของข้อมูล

เมื่อเจ้าของข้อมูลร้องขอเพิกถอนความยินยอม พนักงานที่เกี่ยวข้องและผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องปรึกษากับผู้บริหารและดำเนินการที่จำเป็นเพื่อให้แน่ใจว่าคำขอเพิกถอนได้รับการดำเนินการอย่างเหมาะสมตามที่กำหนดไว้ใน PDPA นโยบาย ระเบียบปฏิบัติและระเบียบปฏิบัติของแผนกนี้

พนักงานที่เกี่ยวข้องและผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องดำเนินการต่อคำขอของเจ้าของข้อมูลภายใน 30 (สามสิบ) วัน และปฏิบัติตามนโยบาย ระเบียบปฏิบัติและระเบียบปฏิบัติของแผนกอื่น ๆ ที่เกี่ยวข้องอย่างเคร่งครัด

5.9 การลบและการทำลายข้อมูล

ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลจะต้องสอดคล้องกับระเบียบปฏิบัติของแผนก อย่างไรก็ตาม ข้อมูลส่วนบุคคลจะไม่ถูกเก็บไว้เกินกว่า 10 (สิบ) ปีในทุกกรณี

พนักงานและผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องลบและทำลายข้อมูลส่วนบุคคลเมื่อข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นอีกต่อไปหรือเมื่อสิ้นสุดระยะเวลาการเก็บรักษาในลักษณะที่ปลอดภัยตามระเบียบปฏิบัติของแผนกที่เกี่ยวข้อง

5.10 มาตรการรักษาความปลอดภัย

5.10.1 แผนก IT ต้องดำเนินการให้แน่ใจว่าไทยยูเนี่ยนมีมาตรการรักษาความปลอดภัยที่เพียงพอ (มาตรการควรครอบคลุมความปลอดภัยที่เกี่ยวข้องทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ ฮาร์ดแวร์ ระบบ และแอพพลิเคชั่น) เพื่อปกป้องข้อมูลส่วนบุคคลอิเล็กทรอนิกส์ตามมาตรฐานสากลและ PDPA

5.10.2 แผนกที่เกี่ยวข้อง/หน่วยบริการร่วม/หน่วยธุรกิจทั้งหมดจะต้องออกและประกาศแนวทางมาตรการรักษาความปลอดภัยสำหรับข้อมูลส่วนบุคคลที่ไม่ใช่อิเล็กทรอนิกส์ที่ได้เก็บรวบรวม ใช้ โอน เปิดเผย ประมวลผล เก็บรักษาและทำลายโดยแผนก/หน่วยบริการร่วม/หน่วยธุรกิจดังกล่าว

5.10.3 พนักงานและผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องปฏิบัติตามรูปแบบการจัดประเภทข้อมูลของไทยยูเนี่ยนอย่างเคร่งครัด ตามที่กำหนดไว้ในนโยบายการรักษาความปลอดภัยของข้อมูลของไทยยูเนี่ยนและระเบียบปฏิบัติของแผนก

6. มาตรการตรวจสอบ

6.1 แผนกที่เกี่ยวข้อง/หน่วยบริการร่วม/หน่วยธุรกิจทั้งหมดจะต้องตรวจสอบให้แน่ใจว่าการดำเนินการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้รับการทำให้เป็นปัจจุบันและแก้ไขให้ถูกต้อง ซึ่งรวมถึงตรวจสอบการเก็บรวบรวม ใช้ การจัดเก็บ ระยะเวลาการเก็บรวบรวม การรักษาความปลอดภัย และการละเมิดข้อมูลส่วนบุคคลเป็นครั้งคราว

6.2 แผนกบริหารความเสี่ยงจะต้องประเมินผลกระทบในการคุ้มครองข้อมูลส่วนบุคคล (DPIA) สำหรับแผนก/หน่วยบริการร่วม/หน่วยธุรกิจที่เกี่ยวข้องทั้งหมดในด้านความเสี่ยงของความเป็นส่วนตัวของข้อมูล ซึ่งมีแนวโน้มที่จะส่งผลให้เกิดความเสี่ยงสูงต่อสิทธิของเจ้าของข้อมูล และเพื่อกำหนดมาตรการที่จำเป็นเพิ่มเติมเพื่อลดความเสี่ยงดังกล่าว

6.3 แผนกตรวจสอบภายในซึ่งเป็นผู้ตรวจสอบภายในจะต้องสุ่มตรวจสอบการควบคุมความปลอดภัยและการปกป้องข้อมูล ซึ่งจะดำเนินการตามการประเมินความเสี่ยงประจำปีเพื่อให้มั่นใจว่าเป็นไปตามนโยบายนี้และข้อกำหนดของ PDPA

7. สิทธิของเจ้าของข้อมูล

7.1 สิทธิในการเพิกถอนความยินยอม

ตามวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมต่อการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิที่จะเพิกถอนความยินยอมได้ทุกเมื่อ

7.2 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิเข้าถึงหรือขอสำเนาข้อมูลส่วนบุคคล ซึ่งไทยยูเนี่ยนได้กำลังเก็บรวบรวม ใช้ และ/หรือเปิดเผย ทั้งนี้เพื่อความเป็นส่วนตัวและการรักษาความปลอดภัย ไทยยูเนี่ยนอาจขอหลักฐานการยืนยันตัวตนของเจ้าของข้อมูลก่อนที่จะส่งมอบข้อมูลส่วนบุคคลตามที่ร้องขอ

7.3 สิทธิในการโอนย้ายข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิได้รับข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ และขอให้ส่งข้อมูลส่วนบุคคลดังกล่าวไปยังผู้ควบคุมข้อมูลรายอื่น โดยที่ (ก) เจ้าของข้อมูลได้ให้ข้อมูลส่วนบุคคลดังกล่าวแก่ไทยยูเนี่ยน และ (ข) ไทยยูเนี่ยนได้เก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลนั้นตามการให้ความยินยอมของเจ้าของข้อมูลหรือวัตถุประสงค์อื่น ๆ ที่ชอบด้วยกฎหมาย

7.4 สิทธิในการคัดค้าน

เจ้าของข้อมูลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลบางอย่างได้

7.5 สิทธิในการลบข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิขอให้ไทยยูเนี่ยนลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนแก่ข้อมูลส่วนบุคคลที่ไทยยูเนี่ยนได้ทำการเก็บรวบรวม ใช้ และ/หรือเปิดเผยได้ เว้นแต่ไทยยูเนี่ยนไม่มีหน้าที่ต้องดำเนินการเช่นนั้น สืบเนื่องจากที่ไทยยูเนี่ยนต้องเก็บข้อมูลส่วนบุคคลเอาไว้เพื่อเป็นการปฏิบัติตามหน้าที่ตามกฎหมายหรือเพื่อดำเนินการ ใช้สิทธิ หรือต่อสู้กับข้อเรียกร้องทางกฎหมาย

7.6 สิทธิในการจำกัดการใช้ข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิจำกัดการใช้ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลเชื่อว่าข้อมูลส่วนบุคคลนั้นไม่ถูกต้อง ซึ่งการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยนั้นไม่ชอบด้วยกฎหมาย หรือข้อมูลส่วนบุคคลนั้นไม่จำเป็นต่อไทยยูเนี่ยนตามวัตถุประสงค์ที่เป็นการเฉพาะเจาะจงอีกต่อไป

7.7 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

เจ้าของข้อมูลมีสิทธิร้องขอให้แก้ไขข้อมูลส่วนบุคคลที่ไม่สมบูรณ์ ไม่ถูกต้อง ที่ทำให้เข้าใจผิด หรือไม่เป็นปัจจุบัน ซึ่งไทยยูเนี่ยนได้เก็บรวบรวม ใช้ และ/หรือเปิดเผย

8. วิธีปฏิบัติเมื่อมีการละเมิดข้อมูลส่วนบุคคล

ในกรณีที่มีการละเมิดการรักษาความปลอดภัยที่นำไปสู่การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคล โดยเหตุบังเอิญหรือไม่ชอบด้วยกฎหมาย พนักงานที่เกี่ยวข้องและผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องแจ้งต่อผู้บริหาร, DPO และส่งอีเมลที่ได้ให้ไว้ในรายละเอียดการติดต่อด้านล่างพร้อมรายละเอียดที่เหมาะสมเกี่ยวกับการละเมิดนั้น**โดยทันทีแต่ไม่เกินกว่า 12 (สิบสอง) ชั่วโมง**

9. ระเบียบปฏิบัติของแผนก

แผนก/หน่วยบริการร่วม/หน่วยธุรกิจทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจะออกและประกาศระเบียบปฏิบัติของแผนก ซึ่งอย่างน้อยระเบียบปฏิบัติของแผนกต้องประกอบด้วยเรื่องดังต่อไปนี้

(1) คำจำกัดความ
(2) บุคคลที่รับผิดชอบของแผนก
(3) การเก็บรวบรวมข้อมูลส่วนบุคคล
(4) แหล่งที่มาของข้อมูลส่วนบุคคล
(5) การแจ้งวัตถุประสงค์และสิทธิในการเก็บรวบรวมข้อมูลส่วนบุคคล
(6) มาตรการป้องกันข้อมูลส่วนบุคคลและมาตรการตรวจสอบภายใน
(7) สิทธิของเจ้าของข้อมูล
(8) ผู้ติดต่อของแผนก
(9) แผนภาพการไหลของข้อมูลและความปลอดภัย

ตัวอย่างระเบียบปฏิบัติของแผนกอยู่ในภาคผนวกที่ 2 ด้านล่าง

10. รายละเอียดการติดต่อ

หากท่านมีคำถามใดๆ เกี่ยวกับนโยบายนี้ โปรดดูรายละเอียดการติดต่อด้านล่าง
อีเมล: PersonalData@ThaiUnion.com

อนุมัติเมื่อวันที่ 26 พฤษภาคม พ.ศ. 2565

-ลงนามโดย-	*-ลงนามโดย-*
(นายธีรพงศ์ จันศิริ)	(นายชู ชง ชาน)
President & CEO	Group Director, Corporate Office

ภาคผนวกที่ 1

แบบฟอร์มคำประกาศเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

สำหรับ [เจ้าของข้อมูล]

[ชื่อบริษัท] ("บริษัท") มีความประสงค์ที่จะแจ้งให้ทราบถึงคำประกาศเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของบริษัทที่เกี่ยวกับ [ชื่อโครงการ] รวมถึงแต่ไม่จำกัดข้อมูลส่วนบุคคลของ [เจ้าของข้อมูล] ซึ่งจะถูกรวบรวม ใช้ และเปิดเผยตามบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ระเบียบการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป กฎหมายและข้อบังคับอื่น ๆ ที่มีผลบังคับใช้ โดยประกาศนี้จะให้ข้อมูลที่สำคัญในขอบเขตดังต่อไปนี้

1. **วัตถุประสงค์ในการรวบรวมข้อมูลส่วนบุคคล**

   บริษัทขอแจ้งวัตถุประสงค์ในการรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

หมายเลข	วัตถุประสงค์ของการดำเนินการ	หลักกฎหมาย
1.	[ถึง/สำหรับ .....] *แจ้งเหตุผลที่จำเป็นต้องรวบรวมหรือเก็บข้อมูล	[หน้าที่ตามกฎหมาย/การปฏิบัติตามสัญญา/เพื่อประโยชน์โดยชอบด้วยกฎหมาย/ความยินยอม] *แจ้งหลักกฎหมายในการดำเนินการนี้ โปรดดูคำอธิบายในหมายเหตุด้านล่าง

2. **ข้อมูลที่ถูกเก็บรวบรวม**

   สำหรับวัตถุประสงค์ตามที่ระบุไว้ข้างต้น บริษัทจำเป็นต้องเก็บรวบรวม ใช้ ประมวลผล และเปิดเผยข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

   - การระบุตัวบุคคล การติดต่อและลักษณะเฉพาะตัว (ตัวอย่างเช่น ชื่อและรายละเอียดการติดต่อ)
   - [รายละเอียดเพิ่มเติมตามความเหมาะสม]

   * แจ้งเกี่ยวกับประเภทของข้อมูลส่วนบุคคลที่รวบรวม ข้อมูลส่วนบุคคลคือข้อมูลใด ๆ ที่สามารถใช้เพื่อระบุตัวบุคคลที่ยังมีชีวิตอยู่ ตัวอย่างเช่น ที่อยู่อีเมลของสมาชิก ข้อมูลทางการเงินของลูกค้า ข้อมูลพนักงาน หรือสถิติผู้ใช้เว็บไซต์

3. **การเก็บรักษา**

   ข้อมูลส่วนบุคคลของท่านจะถูกเก็บรวบรวมไว้เท่าที่จำเป็นตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้แจ้งแก่ท่าน บริษัทจะเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับการทำธุรกรรมของท่านและจะเก็บข้อมูลดังกล่าวไว้ตามระยะเวลาเท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ของการทำธุรกรรมนั้นๆ

4. **การเปิดเผยข้อมูลส่วนบุคคล**

   บริษัทอาจจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของท่านภายในหน่วยงาน และอาจจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของท่านแก่บุคคลภายนอก ทั้งในประเทศไทย [และในประเทศอื่น ๆ (ถ้ามี)] ที่มีมาตรฐานการป้องกันข้อมูลส่วนบุคคลที่เหมาะสม ในกรณีนี้ บริษัทจะจัดให้มีสัญญาที่เหมาะสมเพื่อป้องกันข้อมูลส่วนบุคคลของท่าน

   - [รายชื่อบุคคลภายนอก]

   * แจ้งเกี่ยวกับกรณีต่าง ๆ ที่ส่งข้อมูลส่วนบุคคลไปยังบุคคลภายนอกและสรุปเหตุผลสำหรับการเปิดเผยนี้

5. **การเข้าถึงเว็บไซต์ (ถ้ามี)**

   บริษัทมีหน้าที่ตามกฎหมายของประเทศไทยในการเก็บข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ของท่าน อย่างน้อย ..... (.....) วัน นับแต่วันที่ท่านได้เข้าสู่เว็บไซต์ของบริษัท อย่างไรก็ตาม บริษัทจะไม่ใช้ข้อมูลดังกล่าวเพื่อวิเคราะห์พฤติกรรมการบริโภคหรือทำการวิจัยทางการตลาดโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากท่าน

6. **คุกกี้ (ถ้ามี)**

   คุกกี้คือไฟล์ข้อความขนาดเล็กที่จะถูกเก็บไว้ในเบราว์เซอร์หรืออุปกรณ์ของคอมพิวเตอร์ของท่านเมื่อท่านเชื่อมต่อหรือเยี่ยมชมเว็บไซต์ใดๆ เพื่อนำทางท่านมายังเว็บไซต์ของเรา เพื่อให้ง่ายต่อการใช้งานและมอบบริการที่เป็นส่วนตัวมากขึ้นให้กับท่าน อย่างไรก็ตาม คุกกี้จะไม่เก็บรวบรวมข้อมูลที่อยู่ในคอมพิวเตอร์ของท่าน ("คุกกี้") เพื่อปรับปรุงประสบการณ์ของผู้ใช้เว็บไซต์

   บริษัทใช้คุกกี้เพื่อเรียนรู้เกี่ยวกับสิ่งที่ท่านตอบสนองกับเนื้อหาในเว็บไซต์ของเรา เพื่อมอบความพึงพอใจให้แก่ท่านในระหว่างใช้งานเว็บไซต์ของเรา ซึ่งคุกกี้จะจดจำเบราว์เซอร์ที่ท่านเคยใช้งานและได้รับการติดตั้งในระหว่างที่ท่านอยู่ในเว็บไซต์ของเรา

นอกจากนั้น คุกกี้จะจดจำการตั้งค่าของท่าน เช่นภาษาที่ใช้ ภูมิภาค และการตั้งค่าอัตโนมัติเมื่อท่านกลับเข้ามาเยี่ยมชมเว็บไซต์ของเรา คุกกี้บางชนิดอาจอยู่ตามช่วงเวลาและบางชนิดเป็นคุกกี้ ซึ่งจะถูกเก็บไว้ในคอมพิวเตอร์ของท่านนานขึ้น

สำหรับการดำเนินการบางอย่าง บริษัทจะใช้ผู้ให้บริการภายนอก เช่น การติดตามและวิเคราะห์สถิติการใช้งานและข้อมูลของผู้ใช้งานเว็บไซต์ของบริษัท เพื่อปรับแต่งเว็บไซต์ให้ไปเป็นไปตามสิ่งที่ท่านให้ความสนใจและการดูแลเนื้อหาของเว็บไซต์

บริษัทจะไม่ใช้คุกกี้เพื่อเก็บรวบรวมข้อมูลส่วนบุคคล หากท่านไม่ประสงค์ที่จะรับคุกกี้ ท่านอาจเลือกปฏิเสธคุกกี้หรือบล็อคคุกกี้ที่ส่งมาจากบริษัทหรือผู้ให้บริการภายนอก โดยเปลี่ยนการตั้งค่าในเบราว์เซอร์ของท่าน (ท่านสามารถหาข้อมูลในเมนูให้ความช่วยเหลือของเบราว์เซอร์ของท่าน) อย่างไรก็ตาม เบราว์เซอร์ส่วนใหญ่จะยอมรับคุกกี้โดยอัตโนมัติ หากท่านไม่ประสงค์จะรับคุกกี้ ท่านอาจบล็อกหรือลบคุกกี้ในทันทีได้

7. สิทธิของท่าน

ในความเป็นเจ้าของข้อมูล ท่านมีสิทธิต่างๆดังนี้

- เพิกถอนความยินยอมในการเก็บรวบรวมข้อมูล ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- การขอเข้าถึงและรับสำเนาข้อมูลส่วนบุคคลของท่าน หรือขอให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคลของท่านที่มิได้ให้ความยินยอม
- ขอรับข้อมูลส่วนบุคคลและขอให้โอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอกในกรณีที่สามารถทำได้โดยอัตโนมัติ
- คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ขอให้ลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้
- ขอให้ใช้ข้อมูลส่วนบุคคลโดยเคร่งครัด
- ขอให้ปรับปรุงข้อมูลส่วนบุคคลให้เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด

ท่านสามารถใช้สิทธิของท่านได้โดยส่งอีเมลหรือแจ้งเป็นหนังสือมายังบริษัท โดยแนบบัตรประชาชนของท่านหรือรายละเอียดอื่นๆในลักษณะเดียวกันตามที่บริษัทร้องขอ ซึ่งบริษัทจะดำเนินการตามข้อมูลที่ได้รับเท่าที่ได้รับอนุญาตตามที่กฎหมายกำหนด

โปรดรับทราบว่าบริษัทยังคงสงวนสิทธิของบริษัทตามกฎหมาย ในการปฏิเสธคำขอของท่านในบางกรณี ซึ่งหากบริษัทพิจารณาปฏิเสธคำขอของท่าน ท่านจะได้รับแจ้งถึงเหตุในการปฏิเสธคำขอดังกล่าวนั้น โดยบริษัทจะใช้ความพยายามอย่างดีที่สุดประกอบกับความสามารถในทางเทคนิค ในการตอบคำถามของท่านเกี่ยวกับการดำเนินการข้อมูลส่วนบุคคลของท่าน อย่างไรก็ตาม หากท่านมีข้อกังวลใจ ท่านสามารถติดต่อสอบถาม ร้องเรียนมายังบริษัทหรือดำเนินการกับสำนักงานคุ้มครองข้อมูลส่วนบุคคลต่อไปได้

8. การคุ้มครองข้อมูลส่วนบุคคล

บริษัทให้คำมั่นสัญญาว่าจะปกป้องข้อมูลส่วนบุคคลของท่านภายใต้มาตรฐานการรักษาความปลอดภัย และจะให้การปกป้องข้อมูลส่วนบุคคลของท่านอย่างเหมาะสมเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลจะได้รับการเก็บรวบรวม ถูกใช้หรือเปิดเผยตามกฎหมายและเหมาะสม

9. การแก้ไขเปลี่ยนแปลงแบบแจ้งเกี่ยวกับข้อมูลส่วนบุคคล

บริษัทสงวนสิทธิในการแก้ไขเปลี่ยนแปลงประกาศความเป็นส่วนตัวนี้เพื่อให้เหมาะสมและเป็นไปตามกฎหมาย โปรดตรวจสอบการอัปเดตหรือการแก้ไขเปลี่ยนแปลงประกาศความเป็นส่วนตัวของบริษัทอย่างสม่ำเสมอ

10. การติดต่อ

หากท่านมีข้อสงสัย หรือต้องการใช้สิทธิของท่าน หรือต้องการความช่วยเหลือเกี่ยวกับข้อมูลส่วนบุคคลของท่าน กรุณาส่งอีเมลมายัง [Email] และให้ข้อมูลส่วนบุคคลของท่านพร้อมกับหลักฐานยืนยันตัวตนของท่าน เช่น บัตรประจำตัวประชาชน อย่างไรก็ตาม บริษัทอาจจำเป็นต้องขอเอกสารเพิ่มเติมที่เกี่ยวข้อง หรืออาจปฏิเสธคำขอของท่านหากบริษัทเห็นว่าข้อมูลที่ได้รับมานั้นไม่เพียงพอ

<u>หมายเหตุ</u> คำอธิบายฐานทางกฎหมาย (หลักเกณฑ์ทางกฎหมาย) (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตามมาตรา 24 และมาตรา 26)

1. ***ความยินยอมของเจ้าของข้อมูล***ใช้ในกรณีที่มีข้อมูลที่มีความอ่อนไหวและวัตถุประสงค์นอกเหนือจากข้อ 2 – ข้อ 7 ซึ่งในการให้ความยินยอมนั้น เจ้าของข้อมูลต้องลงนามในแบบฟอร์มให้ความยินยอม
2. ***เพื่อปฏิบัติตามกฎหมาย*** ใช้ในกรณีที่มีความจำเป็นเพื่อปฏิบัติตามกฎหมายตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล
3. ***เพื่อปฏิบัติตามสัญญา*** ใช้ในกรณีการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา หรือเพื่อดำเนินการตามคำขอของเจ้าของข้อมูลก่อนทำสัญญา
4. ***เพื่อประโยชน์โดยชอบด้วยกฎหมาย***ใช้ในกรณีจำเป็นต่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลใดๆ หรือนิติบุคคลใดๆ นอกเหนือไปจากผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ผลประโยชน์นั้นจะถูกแทนที่ด้วยสิทธิขั้นพื้นฐานของเจ้าของข้อมูลดังกล่าวนั้น
5. ***เพื่อประโยชน์สาธารณะ***ใช้ในกรณีความจำเป็นต่อการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือความจำเป็นต่อการใช้สิทธิของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
6. ***ความสำคัญที่เกี่ยวกับชีวิต*** ใช้ในกรณีป้องกันหรือระงับอันตรายแก่ชีวิต ร่างกาย หรือสุขภาพของบุคคล
7. ***การค้นคว้าวิจัยในทางวิทยาศาสตร์/ประวัติศาสตร์*** ใช้ในกรณีที่เกี่ยวกับการจัดเตรียมเอกสารทางประวัติศาสตร์หรือเอกสารสำคัญสำหรับประโยชน์ในทางสาธารณะ หรือเพื่อวัตถุประสงค์ที่เกี่ยวกับการค้นคว้าวิจัยหรือทางสถิติ ซึ่งมาตรการที่เหมาะสมในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลได้มีการจัดเตรียมและเป็นไปตามการแจ้งให้ทราบที่กำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ภาคผนวกที่ 2

แบบฟอร์มและตัวอย่างของระเบียบปฏิบัติของแผนก

1. แบบฟอร์มระเบียบปฏิบัติของแผนก (แบบฟอร์มเปล่า)

ระเบียบปฏิบัติของแผนกในการคุ้มครองข้อมูลส่วนบุคคลสำหรับแผนก ชื่อแผนก

1. คำจำกัดความ

เจ้าของข้อมูล หมายถึง [กรุณาระบุชื่อบุคคลซึ่งข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ถูกใช้ ถูกประมวลผลและถูกเปิดเผย (เช่นลูกค้า ผู้เยี่ยมเยือน ซัพพลายเออร์ และอื่นๆ)]

ข้อมูลส่วนบุคคล หมายถึงข้อมูลใดๆที่เกี่ยวกับตัวบุคคลซึ่งสามารถระบุตัวบุคคลนั้นๆได้ไม่ว่าโดยทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้เสียชีวิต

2. ผู้ที่รับผิดชอบ

[ผู้บริหารแผนก/ หน่วยบริการร่วม/ หน่วยธุรกิจ] ("ผู้บริหาร") คือผู้รับผิดชอบซึ่งดูแลและตรวจสอบการจัดจำแนกประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม ถูกใช้หรือถูกเปิดเผยตามวัตถุประสงค์ที่ได้แจ้งไว้แก่ลูกค้า รวมถึงการจัดเตรียมมาตรการรักษาความปลอดภัยให้แก่ข้อมูลและมาตรการตรวจสอบ เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นได้รับการอัปเดต ถูกต้องและเที่ยงตรง ผู้บริหารต้องแต่งตั้งผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลเป็นผู้ช่วยในการกำกับดูแลข้อมูลส่วนบุคคลของ [...]

3. การเก็บรวบรวมข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องเป็นตามวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูลเท่านั้น ซึ่งไทยยูเนี่ยนจะไม่เก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวซึ่งอาจก่อให้เกิดการเลือกปฏิบัติหรือความไม่ยุติธรรมต่อเจ้าของข้อมูล โดยไม่ได้รับความยินยอมโดยเปิดเผยจากเจ้าของข้อมูลเหล่านั้น เว้นแต่จะเป็นการเก็บรวบรวมตามกฎหมาย PDPA

ไทยยูเนี่ยนจะเก็บรวบรวมข้อมูลส่วนบุคคลเช่น [ประเภทของข้อมูลส่วนบุคคล เช่นชื่อ เบอร์โทรศัพท์] เพื่อ [วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล]

การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องเป็นไปตาม (1) เพื่อปฏิบัติตามสัญญาเพื่อการเริ่มหรือการปฏิบัติตามสัญญาต่อลูกค้า (2) เพื่อปฏิบัติตามกฎหมาย เพื่อการปฏิบัติตามหน้าที่ตามกฎหมาย (3)เพื่อประโยชน์โดยชอบด้วยกฎหมายเพื่อวัตถุประสงค์ของผลประโยชน์ที่ชอบด้วยกฎหมายและประโยชน์ที่ชอบด้วยกฎหมายของบุคคลภายนอก ซึ่งไทยยูเนี่ยนจะรักษาสมดุลของประโยชน์ที่ชอบด้วยกฎหมายตามประโยชน์ สิทธิขั้นพื้นฐานและเสรีภาพของไทยยูเนี่ยนและของ [...] ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของ [...] (4) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างการหรือสุขภาพของบุคคล และ/หรือ (5) เพื่อประโยชน์สาธารณะ เพื่อการปฏิบัติหน้าที่สำหรับประโยชน์ในทางสาธารณะ หรือเพื่อการใช้สิทธิของเจ้าหน้าที่ของรัฐ (6) สำหรับการดำเนินการและการใช้สิทธิเรียกร้องทางกฎหมายหรือที่ได้รับอนุญาตตามกฎหมายอื่นภายใต้กฎหมายที่บังคับใช้ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (ตามแต่กรณี) ซึ่งไทยยูเนี่ยนอาจเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งเป็นไปตามบริบทของความสัมพันธ์ของไทยยูเนี่ยน ตามวัตถุประสงค์ดังต่อไปนี้

1) .....
2) .....
3) .....
4) .....
5) .....

4. ที่มาของข้อมูลส่วนบุคคล

การรับข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลตามวิธีการดังต่อไปนี้

ก) .....
ข) .....

5. การแจ้งวัตถุประสงค์ของการเก็บรวบรวมและสิทธิที่เกี่ยวข้อง

เจ้าของข้อมูลจะได้รับแจ้งถึงวัตถุประสงค์ในการเก็บรวมรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลของพวกเขา พร้อมกันกับเงื่อนไขและสิทธิและการขอความยินยอม (ถ้ามี) ก่อนการเก็บรวบรวม ประมวลผลหรือเปิดเผยข้อมูลโดย.....

6. มาตรการป้องกันข้อมูลส่วนบุคคลรวมถึงมาตรการตรวจสอบภายใน

6.1 วัตถุประสงค์

เจ้าของข้อมูลจะถูกเก็บรวบรวมและถูกใช้ข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์ที่ได้รับแจ้งเอาไว้

6.2 การเก็บรักษา

ก) โดยรูปแบบเอกสาร (Hard Copy): .....

ข) โดยรูปแบบอิเล็กทรอนิกส์ (Soft Copy): .....

6.3 ขั้นตอนการเก็บรวบรวม: ข้อจำกัดของการเก็บรวบรวมข้อมูลส่วนบุคคลจะถูกจำกัดไว้ดังต่อไปนี้

ก) เก็บรวบรวมทั้งรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์เพื่อตรวจสอบการระบุตัวตน เช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อีเมล หลักฐานอื่นๆที่ร้องขอในระหว่างการเตรียมเก็บรวบรวมจนกว่าจะทำสัญญา

ข) เก็บรวบรวมทั้งรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์เพื่อตรวจสอบการระบุตัวตนสำหรับการดำเนินการต่อผลิตภัณฑ์/การให้บริการ เช่นการเข้าเยี่ยมชมสถานที่ (ถ้ามี) ก่อนเริ่มโครงการ/การดำเนินการทางธุรกิจ

ค) เก็บรวบรวมข้อมูลจำเพาะของลูกค้า สิ่งที่ร้องขอเพิ่มเติมหรือการแก้ไขขอบเขตการให้บริการ (ถ้ามี) สำหรับการดำเนินโครงการ/การดำเนินการทางธุรกิจ

6.4 เมื่อระยะเวลาในการเก็บรวบรวมข้อมูลสิ้นสุดลง หรือไทยยูเนี่ยน ไม่มีสิทธิ หรือไม่มีวัตถุประสงค์โดยชอบด้วยกฎหมายในการดำเนินการต่อข้อมูลส่วนบุคคลของลูกค้า ไทยยูเนี่ยนจะดำเนินการทำลายและลบข้อมูลส่วนบุคคล ซึ่งเอกสารที่เกี่ยวกับข้อมูลส่วนบุคคลจะถูกทำลายด้วยเครื่องย่อยเอกสารและข้อมูลส่วนบุคคลที่เป็นอิเล็กทรอนิกส์จะถูกลบออกจากระบบ

6.5 การดำเนินการกับข้อมูลส่วนบุคคล

เมื่อได้รับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลจะถูกดำเนินการดังต่อไปนี้

❒ การเก็บรวบรวม: พนักงานที่เกี่ยวข้องจะเก็บรักษาข้อมูลส่วนบุคคลเอาไว้ในไฟล์หรือแฟ้มเป็นการเฉพาะเจาะจง และจะดูแลรักษาให้เป็นไปตามข้อ 6.6 [และหากมีการส่งต่อ/แบ่งปันไปยังแผนกอื่นๆเป็นการภายใน กรุณาระบุ]

❒ การใช้: พนักงานที่เกี่ยวข้องจะใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้รับแจ้งให้ทราบ

❒ การเปิดเผยต่อบุคคลภายนอก เช่น [หากมีการส่งต่อ/แบ่งปันไปยังบุคคลอื่นเพื่อดำเนินการ กรุณาระบุ] ต้องทำสัญญา NDA และ DPA ก่อนการเปิดเผยข้อมูล

6.6 ระยะเวลาการเก็บรวบรวม

ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลเอาไว้เป็นเวลา .... (....) ปี นับจากการบอกเลิกหรือการสิ้นสุดของสัญญา และจะลบ/ทำลายข้อมูลส่วนบุคคลภายใน .... (....) วัน หลังจากระยะเวลาการเก็บรวบรวมดังกล่าว

6.7 การรักษาความปลอดภัย

ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะรักษามาตรการรักษาความปลอดภัยที่เหมาะสม ซึ่งรวมถึงการบริหารจัดการการป้องกันทางเทคนิคและทางกายภาพที่เกี่ยวกับการควบคุมการเข้าถึง เพื่อเป็นการป้องกันความลับ ความมั่นคงและความพร้อมในการใช้ข้อมูลส่วนบุคคล จากความสูญเสีย การปรับเปลี่ยน การแก้ไข การใช้หรือการเข้าถึงโดยเหตุบังเอิญ โดยผิดกฎหมายหรือมิได้รับอนุญาตให้สอดคล้องกับกฎหมายที่บังคับใช้ โดยเฉพาะอย่างยิ่ง การใช้มาตรการควบคุมการเข้าถึง ซึ่งปลอดภัยและเหมาะสมต่อการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล และการเข้าถึงที่เข้มงวดไปยังข้อมูลส่วนบุคคลของเจ้าของข้อมูล เช่นเดียวกับการเก็บรักษาและอุปกรณ์ประมวลผลโดยการกำหนดการให้สิทธิหรืออนุญาตให้เข้าถึง ผู้ใช้งาน การควบคุมการเข้าถึงเพื่อจำกัดการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้แก่ผู้ที่ได้รับอนุญาตเท่านั้น และแต่งตั้งผู้ใช้งานที่รับผิดชอบในการป้องกันการเข้าถึงที่มิได้รับอนุญาต การเปิดเผย การรับรู้ การทำซ้ำข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่ผิดกฎหมาย หรือการโจรกรรมอุปกรณ์ที่ใช้จัดเก็บและประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล ซึ่งรวมถึงมาตรการที่สามารถทำการตรวจสอบซ้ำถึงการเข้าถึง การแก้ไข การลบหรือการส่งข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่มิได้รับอนุญาต ซึ่งเหมาะสมกับวิธีการและวัตถุประสงค์ของการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล

6.8 มาตรการตรวจสอบ

ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องคอยตรวจสอบและควบคุมเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นเป็นปัจจุบันและถูกต้องเที่ยงตรง รวมถึงการตรวจสอบการเก็บรวบรวม การใช้ การเก็บรักษา ระยะเวลาการเก็บรวบรวม การรักษาความปลอดภัยและการละเมิดต่อข้อมูลส่วนบุคคลเป็นครั้งคราว

หากเจ้าของข้อมูลประสงค์จะอัปเดทข้อมูลส่วนบุคคลในระหว่างการประมวลผลข้อมูลส่วนบุคคล ไทยยูเนี่ยนจะทำการอัปเดทข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้ถูกต้องและเป็นข้อมูลปัจจุบันตามที่ได้รับแจ้ง

6.9 การรั่วไหลของข้อมูล

ในกรณีของการรั่วไหลของข้อมูลที่นำไปสู่การทำลาย ความสูญหาย การแก้ไขที่ไม่ได้ตั้งใจหรือโดยผิดกฎหมาย การเปิดเผยหรือการเข้าถึงข้อมูลส่วนบุคคลที่มิได้รับอนุญาต ผู้ใช้งานหรือผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกต้องแจ้งผู้จัดการในสายงานโดยทันทีหรือไม่เกินกว่า 12 ชั่วโมง และรายงานถึงไทยยูเนี่ยนโดยทางอีเมลที่ได้ระบุไว้ในรายละเอียดการติดต่อด้านล่างถึงเหตุการณ์ที่เกิดขึ้นพร้อมกับรายละเอียดที่เหมาะสม

7. สิทธิของเจ้าของข้อมูล

7.1 สิทธิในการเพิกถอนการให้ความยินยอม: ตามวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมต่อการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิที่จะเพิกถอนความยินยอมได้ทุกเมื่อ

7.2 สิทธิในการเข้าถึง: เจ้าของข้อมูลมีสิทธิเข้าถึงหรือขอสำเนาข้อมูลส่วนบุคคล ซึ่งไทยยูเนี่ยนได้กำลังเก็บรวบรวม ใช้ และ/หรือเปิดเผย ทั้งนี้เพื่อความเป็นส่วนตัวและการรักษาความปลอดภัย ไทยยูเนี่ยนอาจขอหลักฐานการยืนยันตัวตนของเจ้าของข้อมูลก่อนที่จะส่งมอบข้อมูลส่วนบุคคลตามที่ร้องขอ

7.3 สิทธิในการโอนย้ายข้อมูล: เจ้าของข้อมูลมีสิทธิได้รับข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ และขอให้ส่งข้อมูลส่วนบุคคลดังกล่าวไปยังผู้ควบคุมข้อมูลรายอื่น โดยที่ (ก) เจ้าของข้อมูลได้ให้ข้อมูลส่วนบุคคลดังกล่าวแก่ไทยยูเนี่ยน และ (ข) ไทยยูเนี่ยนได้เก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลนั้นตามการให้ความยินยอมของเจ้าของข้อมูลหรือวัตถุประสงค์อื่น ๆ ที่ชอบด้วยกฎหมาย

7.4 สิทธิในการคัดค้าน: เจ้าของข้อมูลมีสิทธิคัดค้านการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคลบางอย่างได้

7.5 สิทธิในการลบข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิขอให้ไทยยูเนี่ยนลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนแก่ข้อมูลส่วนบุคคลที่ไทยยูเนี่ยนได้ทำการเก็บรวบรวม ใช้ และ/หรือเปิดเผยได้ เว้นแต่ไทยยูเนี่ยนไม่มีหน้าที่ต้องดำเนินการเช่นนั้น สืบเนื่องจากที่ไทยยูเนี่ยนต้องเก็บข้อมูลส่วนบุคคลเอาไว้เพื่อเป็นการปฏิบัติตามหน้าที่ตามกฎหมายหรือเพื่อดำเนินการ ใช้สิทธิ หรือต่อสู้กับข้อเรียกร้องทางกฎหมาย

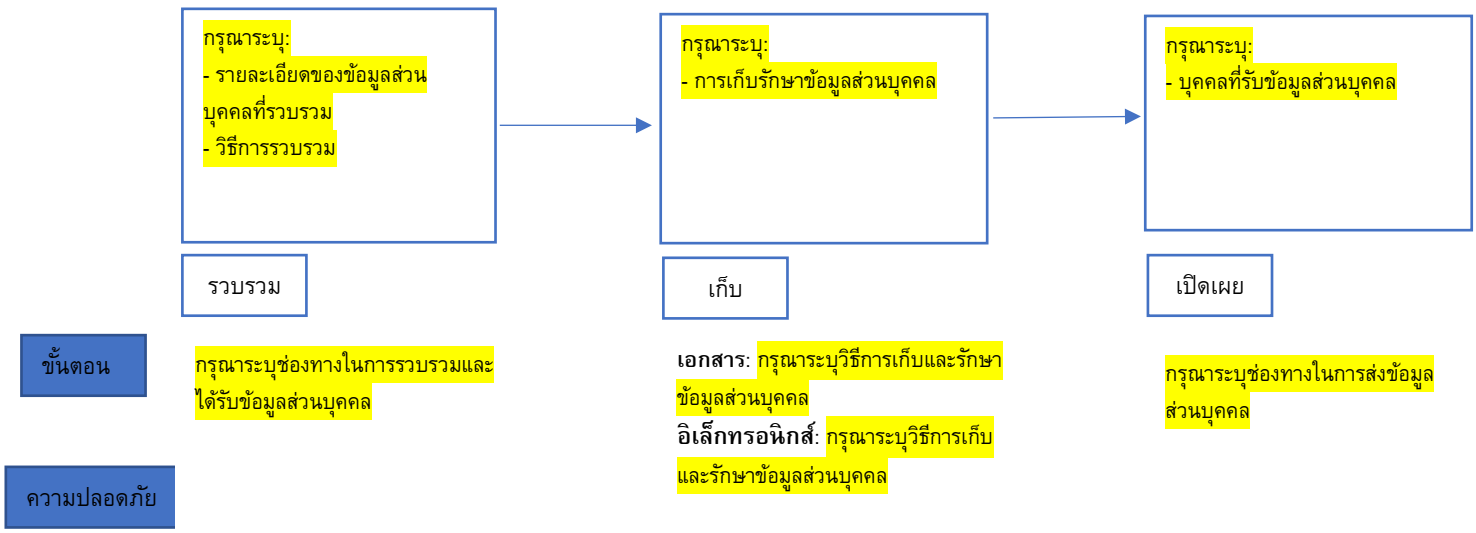
7.6 สิทธิการขอให้แก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง: เจ้าของข้อมูลมีสิทธิร้องขอให้แก้ไขข้อมูลส่วนบุคคลที่ไม่สมบูรณ์ ไม่ถูกต้อง ที่ทำให้เข้าใจผิด หรือไม่เป็นปัจจุบัน ซึ่งไทยยูเนี่ยนได้เก็บรวบรวม ใช้ และ/หรือเปิดเผย

7.7 สิทธิในการจำกัดการใช้ข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิจำกัดการใช้ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลเชื่อว่าข้อมูลส่วนบุคคลนั้นไม่ถูกต้อง ซึ่งการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยนั้นไม่ชอบด้วยกฎหมาย หรือข้อมูลส่วนบุคคลนั้นไม่จำเป็นต่อไทยยูเนี่ยนตามวัตถุประสงค์ที่เป็นการเฉพาะเจาะจงอีกต่อไป

8. ผู้ติดต่อ

ผู้รับผิดชอบ/ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนก
ชื่อ.....
อีเมล.....
หมายเลขโทรศัพท์.....

9. การไหลของข้อมูลและความปลอดภัย



2. ตัวอย่างระเบียบปฏิบัติของแผนกสำหรับการคุ้มครองข้อมูลส่วนบุคคลของแผนกการตลาด

1. คำจำกัดความ

ลูกค้า หมายถึงบุคคลซึ่งซื้อผลิตภัณฑ์และ/หรือใช้บริการของไทยยูเนี่ยน และ/หรือผู้ที่คาดว่าจะซื้อผลิตภัณฑ์และ/หรือใช้บริการของไทยยูเนี่ยน (ลูกค้าในอนาคต) ซึ่งรวมถึงผู้ที่เกี่ยวข้องหรือเป็นตัวแทนของลูกค้า เช่น ผู้บริหาร กรรมการ พนักงาน ตัวแทนหรือนิติบุคคลของลูกค้า รวมถึงผู้ที่มีข้อมูลส่วนบุคคลปรากฏอยู่ในเอกสารและการประมวลผลที่เกี่ยวข้อง เช่น ผู้จัดการ ผู้จัดซื้อ ผู้รับสินค้า และผู้สั่งจ่ายเช็คธนาคาร และอื่นๆ

ข้อมูลส่วนบุคคล หมายถึงข้อมูลใดๆที่เกี่ยวข้องกับบุคคลซึ่งสามารถระบุตัวตนได้ ไม่ว่าโดยทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ที่เสียชีวิต

2. ผู้รับผิดชอบ

ผู้จัดการทั่วไปของแผนกการตลาด ("ผู้บริหาร") เป็นผู้รับผิดชอบในการดูแลและทำให้แน่ใจว่าข้อมูลส่วนบุคคลที่ได้รับการจำแนกประเภทได้ถูกเก็บรวบรวม ถูกใช้หรือถูกเปิดเผยนั้น เป็นไปตามวัตถุประสงค์ที่ได้แจ้งไว้กับลูกค้า ซึ่งรวมถึงการจัดให้มีมาตรการรักษาความปลอดภัยและการตรวจสอบเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นเป็นปัจจุบัน ถูกต้องและเที่ยงตรง
หัวหน้าหน่วยงานจะต้องแต่งตั้งผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกเพื่อให้ความช่วยเหลือในการกำกับดูแลข้อมูลส่วนบุคคล

3. การเก็บรวบรวมข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องเป็นไปตามวัตถุประสงค์ที่ได้รับแจ้งจากลูกค้าเท่านั้น (เจ้าของข้อมูล)
ไทยยูเนี่ยนจะไม่เก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวซึ่งอาจก่อให้เกิดการเลือกปฏิบัติหรือความไม่ยุติธรรมต่อเจ้าของข้อมูล โดยไม่ได้รับความยินยอมโดยเปิดเผยจากเจ้าของข้อมูลเหล่านั้น เว้นแต่จะเป็นการเก็บรวบรวมตามกฎหมาย PDPA
ไทยยูเนี่ยนจะเก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นต่อการยืนยันตัวตนและเพื่อการกำกับดูแลผลิตภัณฑ์/การให้บริการ เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล คำร้องของลูกค้า ใบเรียกเก็บเงินสำหรับการทำสัญญา และการดำเนินการอื่นๆที่เกี่ยวข้องเท่านั้น เช่น การตรวจสอบหลักฐานในการทำสัญญา การพิจารณาวงเงิน การให้หลักประกัน และอื่นๆ
การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องเป็นไปตาม (1) เพื่อปฏิบัติตามสัญญาเพื่อการเริ่มหรือการปฏิบัติตามสัญญาต่อลูกค้า (2) เพื่อปฏิบัติตามกฎหมาย เพื่อการปฏิบัติตามหน้าที่ตามกฎหมาย (3)เพื่อประโยชน์โดยชอบด้วยกฎหมายเพื่อวัตถุประสงค์ของผลประโยชน์ที่ชอบด้วยกฎหมายและประโยชน์ที่ชอบด้วยกฎหมายของบุคคลภายนอก ซึ่งไทยยูเนี่ยนจะรักษาสมดุลของประโยชน์ที่ชอบด้วยกฎหมายตามประโยชน์ สิทธิขั้นพื้นฐานและเสรีภาพของไทยยูเนี่ยนและของลูกค้า ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของลูกค้า (4) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างการหรือสุขภาพของบุคคล และ/หรือ (5) เพื่อประโยชน์สาธารณะ เพื่อการปฏิบัติหน้าที่สำหรับประโยชน์ในทางสาธารณะ หรือเพื่อการใช้สิทธิของเจ้าหน้าที่ของรัฐ (6) สำหรับการดำเนินการและการใช้สิทธิเรียกร้องทางกฎหมายหรือที่ได้รับอนุญาตตามกฎหมายอื่นภายใต้กฎหมายที่บังคับใช้ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (ตามแต่กรณี) ซึ่งไทยยูเนี่ยนอาจเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งเป็นไปตามบริบทของความสัมพันธ์ของไทยยูเนี่ยน ตามวัตถุประสงค์ดังต่อไปนี้

1) เพื่อการดำเนินธุรกิจของไทยยูเนี่ยน
2) เพื่อลงทะเบียนและตรวจสอบ
3) เพื่อการสื่อสารในทางการตลาด
4) เพื่อพัฒนาการดำเนินธุรกิจ ผลิตภัณฑ์และการให้บริการ
5) เพื่อปฏิบัติตามหน้าที่ตามกฎหมายและคำสั่งของหน่วยงานของรัฐ

4. ที่มาของข้อมูลส่วนบุคคล

การรับข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลตามวิธีการดังต่อไปนี้

ก) เมื่อลูกค้ามีส่วนร่วมในการสื่อสารหรือสอบถาม แสดงความคิดเห็น หรือตอบกลับมายังไทยยูเนี่ยน ไม่ว่าจะเป็นลายลักษณ์อักษรหรือโดยทางวาจาผ่านเว็บไซต์ แอพพลิเคชั่น โดยทางโทรศัพท์ อีเมล แฟกซ์ การสื่อสารแบบเผชิญหน้า (face-to-face interaction) หรือ โดยวิธีการอื่น และ/หรือ
ข) เมื่อลูกค้าแสดงความประสงค์ว่าจะซื้อผลิตภัณฑ์หรือใช้บริการของไทยยูเนี่ยน ทำสัญญากับไทยยูเนี่ยน หรือส่งมอบเอกสารเกี่ยวกับข้อมูลส่วนบุคคลให้แก่ไทยยูเนี่ยน

5. การแจ้งถึงวัตถุประสงค์และสิทธิของการเก็บรวบรวม

ลูกค้าจะได้รับแจ้งเกี่ยวกับวัตถุประสงค์ของการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลของลูกค้า พร้อมๆกับเงื่อนไข สิทธิ และการขอการให้ความยินยอม (ถ้ามี) ก่อนการเก็บรวบรวม การประมวลผลหรือการเปิดเผย โดยส่งไปพร้อมกันกับสัญญา ใบเสนอราคา ข้อเสนอ และอื่นๆ

6. มาตรการป้องกันข้อมูลส่วนบุคคลรวมถึงมาตรการตรวจสอบภายใน

6.1 วัตถุประสงค์

ข้อมูลส่วนบุคคลของลูกค้าจะถูกเก็บรวบรวมและถูกใช้ข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์ที่ได้รับแจ้งเอาไว้

6.2 การเก็บรักษา

ก) โดยรูปแบบเอกสาร (Hard Copy): เอกสารของลูกค้า เช่น สำเนาบัตรประจำตัวประชาชน สำเนาหนังสือเดินทาง สำเนาทะเบียนบ้าน ข้อมูลจำเพาะที่ลูกค้าต้องการ (requirement specification) จะถูกเก็บรักษาอยู่ในไฟล์รายชื่อลูกค้าที่ปลอดภัย

ข) โดยรูปแบบอิเล็กทรอนิกส์ (Soft Copy): เอกสารของลูกค้า เช่น ไฟล์ pdf จะถูกเก็บรักษาไว้ในโฟลเดอร์รายชื่อลูกค้า

6.3 ขั้นตอนการเก็บรวบรวม: ข้อจำกัดการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าจะถูกจำกัดไว้ดังต่อไปนี้

ก) เก็บรวบรวมทั้งในรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์เพื่อการยืนยันตัวตน เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล หลักฐานอื่นๆที่ร้องขอในระหว่างการเตรียมเก็บรวบรวมจนกว่าจะทำสัญญา

ข) เก็บรวบรวมทั้งในรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์เพื่อการยืนยันตัวตนสำหรับการการดำเนินการต่อผลิตภัณฑ์/การให้บริการ เช่นการเข้าเยี่ยมชมสถานที่ (ถ้ามี) ก่อนเริ่มโครงการ/การดำเนินการทางธุรกิจ

ค) เก็บรวบรวมข้อมูลจำเพาะของลูกค้า สิ่งที่ร้องขอเพิ่มเติมหรือการแก้ไขขอบเขตการให้บริการ (ถ้ามี) สำหรับการดำเนินโครงการ/การดำเนินการทางธุรกิจ

6.4 เมื่อระยะเวลาในการเก็บรวบรวมข้อมูลสิ้นสุดลง หรือไทยยูเนี่ยน ไม่มีสิทธิ หรือไม่มีวัตถุประสงค์โดยชอบด้วยกฎหมายในการดำเนินการต่อข้อมูลส่วนบุคคลของลูกค้า ไทยยูเนี่ยนจะดำเนินการทำลายและลบข้อมูลส่วนบุคคล ซึ่งเอกสารที่เกี่ยวกับข้อมูลส่วนบุคคลจะถูกทำลายด้วยเครื่องย่อยเอกสารและข้อมูลส่วนบุคคลที่เป็นอิเล็กทรอนิกส์จะถูกลบออกจากระบบ

6.5 การดำเนินการกับข้อมูลส่วนบุคคล

เมื่อได้รับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลจะถูกดำเนินการดังต่อไปนี้

❒ การเก็บรวบรวม: พนักงานที่เกี่ยวข้องจะเก็บรักษาข้อมูลส่วนบุคคลเอาไว้ในไฟล์หรือแฟ้มเป็นการเฉพาะเจาะจง และจะดูแลรักษาให้เป็นไปตามข้อ 6.6 และส่งต่อไปยังแผนกบัญชีเพื่อออกใบเสร็จ

❒ การใช้: พนักงานที่เกี่ยวข้องจะใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้รับแจ้งให้ทราบ

❒ การเปิดเผยต่อบุคคลภายนอก เช่น ผู้ให้บริการ สายการบิน โรงแรมที่พักและอื่นๆ ต้องทำสัญญา NDA และ DPA ก่อนการเปิดเผยข้อมูล

6.6 ระยะเวลาการเก็บรวบรวม

ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลเอาไว้เป็นเวลา .... (....) ปี นับจากการบอกเลิกหรือการสิ้นสุดของสัญญา และจะลบ/ทำลายข้อมูลส่วนบุคคลภายใน 30 (สามสิบ) วัน หลังจากระยะเวลาการเก็บรวบรวมดังกล่าว

6.7 การรักษาความปลอดภัย

ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะรักษามาตรการรักษาความปลอดภัยที่เหมาะสม ซึ่งรวมถึงการบริหารจัดการการป้องกันทางเทคนิคและทางกายภาพที่เกี่ยวกับการควบคุมการเข้าถึง เพื่อเป็นการป้องกันความลับ ความมั่นคงและความพร้อมในการใช้ข้อมูลส่วนบุคคล จากความสูญเสีย การปรับเปลี่ยน การแก้ไข การใช้หรือการเข้าถึงโดยเหตุบังเอิญ โดยผิดกฎหมายหรือมิได้รับอนุญาตให้สอดคล้องกับกฎหมายที่บังคับใช้ โดยเฉพาะอย่างยิ่ง การใช้มาตรการควบคุมการเข้าถึง ซึ่งปลอดภัยและเหมาะสมต่อการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้า และการเข้าถึงที่เข้มงวดไปยังข้อมูลส่วนบุคคลของลูกค้า เช่นเดียวกับการเก็บรักษาและอุปกรณ์ประมวลผลโดยการกำหนดการให้สิทธิหรืออนุญาตให้เข้าถึงผู้ใช้งาน การควบคุมการเข้าถึงเพื่อจำกัดการเข้าถึงข้อมูลส่วนบุคคลของลูกค้าให้แก่ผู้ที่ได้รับอนุญาตเท่านั้น และแต่งตั้งผู้ใช้งานที่รับผิดชอบในการป้องกันการเข้าถึงที่มิได้รับอนุญาต การเปิดเผย การรับรู้ การทำซ้ำข้อมูลส่วนบุคคลของลูกค้าที่ผิดกฎหมายหรือการโจรกรรมอุปกรณ์ที่ใช้จัดเก็บและประมวลผลข้อมูลส่วนบุคคลของลูกค้า ซึ่งรวมถึง มาตรการที่สามารถทำการตรวจสอบซ้ำถึงการเข้าถึง การแก้ไข การลบหรือการส่งข้อมูลส่วนบุคคลของลูกค้าที่มิได้รับอนุญาต ซึ่งเหมาะสมกับวิธีการและวัตถุประสงค์ของการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคลของลูกค้า

6.8 มาตรการตรวจสอบ

ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกจะต้องคอยตรวจสอบและควบคุมเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นเป็นปัจจุบันและถูกต้องเที่ยงตรง รวมถึงการตรวจสอบการเก็บรวบรวม การใช้ การเก็บรักษา ระยะเวลาการเก็บรวบรวม การรักษาความปลอดภัยและการละเมิดต่อข้อมูลส่วนบุคคลเป็นครั้งคราว

หากลูกค้าประสงค์จะอัปเดทข้อมูลส่วนบุคคลในระหว่างการประมวลผลข้อมูลส่วนบุคคล ไทยยูเนี่ยนจะทำการอัปเดทข้อมูลส่วนบุคคลของลูกค้าให้ถูกต้องและเป็นข้อมูลปัจจุบันตามที่ได้รับแจ้ง

6.9 การรั่วไหลของข้อมูล

ในกรณีของการรั่วไหลของข้อมูลที่นำไปสู่การทำลาย ความสูญหาย การแก้ไขที่ไม่ได้ตั้งใจหรือโดยผิดกฎหมาย การเปิดเผยหรือการเข้าถึงข้อมูลส่วนบุคคลที่มิได้รับอนุญาต ผู้ใช้งานหรือผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนกต้องแจ้งผู้จัดการในสายงานโดยทันทีหรือไม่เกินกว่า 12 ชั่วโมง และรายงานถึงไทยยูเนี่ยนโดยทางอีเมลที่ได้ระบุไว้ในรายละเอียดการติดต่อด้านล่างถึงเหตุการณ์ที่เกิดขึ้นพร้อมกับรายละเอียดที่เหมาะสม

7. สิทธิของเจ้าของข้อมูล

7.1 สิทธิในการเพิกถอนการให้ความยินยอม: ตามวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมต่อการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิที่จะเพิกถอนความยินยอมได้ทุกเมื่อ

7.2 สิทธิในการเข้าถึง: เจ้าของข้อมูลมีสิทธิเข้าถึงหรือขอสำเนาข้อมูลส่วนบุคคล ซึ่งไทยยูเนี่ยนได้กำลังเก็บรวบรวม ใช้ และ/หรือเปิดเผย ทั้งนี้เพื่อความเป็นส่วนตัวและการรักษาความปลอดภัย ไทยยูเนี่ยนอาจขอหลักฐานการยืนยันตัวตนของเจ้าของข้อมูลก่อนที่จะส่งมอบข้อมูลส่วนบุคคลตามที่ร้องขอ

7.3 สิทธิในการโอนย้ายข้อมูล: เจ้าของข้อมูลมีสิทธิได้รับข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ และขอให้ส่งข้อมูลส่วนบุคคลดังกล่าวไปยังผู้ควบคุมข้อมูลรายอื่น โดยที่ (ก) เจ้าของข้อมูลได้ให้ข้อมูลส่วนบุคคลดังกล่าวแก่ไทยยูเนี่ยน และ (ข) ไทยยูเนี่ยนได้เก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลนั้นตามการให้ความยินยอมของเจ้าของข้อมูลหรือวัตถุประสงค์อื่น ๆ ที่ชอบด้วยกฎหมายในการโอนย้ายข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิได้รับข้อมูลส่วนบุคคลในรูปแบบอีเล็กทรอนิกส์ที่ถูกสร้างขึ้น และส่งมอบข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลอีกคนหนึ่งได้ ตามที่ (ก) เจ้าของข้อมูลได้ส่งมอบข้อมูลส่วนบุคคลแก่ไทยยูเนี่ยน และ (ข) หากไทยยูเนี่ยนได้ทำการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลนั้นตามการให้ความยินยอมของเจ้าของข้อมูลหรือตามวัตถุประสงค์โดยชอบด้วยกฎหมาย

7.4 สิทธิในการคัดค้าน: เจ้าของข้อมูลมีสิทธิคัดค้านการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคลบางอย่างได้

7.5 สิทธิในการลบข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิขอให้ไทยยูเนี่ยนลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนแก่ข้อมูลส่วนบุคคลที่ไทยยูเนี่ยนได้ทำการเก็บรวบรวม ใช้ และ/หรือเปิดเผยได้ เว้นแต่ไทยยูเนี่ยนไม่มีหน้าที่ต้องดำเนินการเช่นนั้น สืบเนื่องจากที่ไทยยูเนี่ยนต้องเก็บข้อมูลส่วนบุคคลเอาไว้เพื่อเป็นการปฏิบัติตามหน้าที่ตามกฎหมายหรือเพื่อดำเนินการ ใช้สิทธิ หรือต่อสู้กับข้อเรียกร้องทางกฎหมาย

7.6 สิทธิการขอให้แก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง: เจ้าของข้อมูลมีสิทธิร้องขอให้แก้ไขข้อมูลส่วนบุคคลที่ไม่สมบูรณ์ ไม่ถูกต้อง ที่ทำให้เข้าใจผิด หรือไม่เป็นปัจจุบัน ซึ่งไทยยูเนี่ยนได้เก็บรวบรวม ใช้ และ/หรือเปิดเผย

7.7 สิทธิในการจำกัดการใช้ข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิจำกัดการใช้ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลเชื่อว่าข้อมูลส่วนบุคคลนั้นไม่ถูกต้อง ซึ่งการเก็บรวบรวม การใช้ และ/หรือการเปิดเผยนั้นไม่ชอบด้วยกฎหมาย หรือข้อมูลส่วนบุคคลนั้นไม่จำเป็นต่อไทยยูเนี่ยนตามวัตถุประสงค์ที่เป็นการเฉพาะเจาะจงอีกต่อไป

8. ผู้ติดต่อ

ผู้รับผิดชอบ/ผู้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของแผนก

ชื่อ: .....

อีเมล: .....

หมายเลขโทรศัพท์: .....

9. แผนภาพการไหลของข้อมูลและความปลอดภัย