Data Protection Policy

Summary

This Document sets expectation for how the personal information of our customers, business partners, employees or those involved in the business of the company will be treated confidentially.

Application field

This document applies to then entire company.

Identification

Document Number: TE-HR-P-07 Revision Level: A

Department Owner: Top Management

Reviewing and Approval process

Reviewed by:

Name	Function	Signature
Napa S.	GM	Approved

Approved by:

Name	Function	Date of last version	Signature
Laurent L.	MD	10/04/2020	Approved

REVISION LIST

Revision Level	List of Changes
A	**First Issue**

PLAN

Contents

I. Purpose

To provide the personal information of customers, partners, visitors, employees, or those who involved in the company's businesses are treated confidentially and used as the data owners consent. The company therefore stipulates the regulations for related parties to strictly follow.

II. Scope

The content of this document applies to all employees of the company.

III. Responsibility and Authority

All employees are in charge of:

- Reading and understanding for company policies
- Annual acknowledgement of the company policies especially for the processing employees
- Agreed and followed all company policies

IV. Reporting

All Thai Ecotrade staffs must know and understand all company policies and have duty to follow all requirements. All employees must know all company policies and need to sign an Employee Acknowledgement Form once he/she was joined Thai Ecotrade. Additionally, all drivers and destruction processing employee files must contain an annual Acknowledgement of the company's written policies.

V. Objectives

GOAL:	Data Protection Policy Awareness to all employees	
Success Factor:	All employees know and understand this policy	
KPI	Number of employees act and follow the policies	
Definition	Make sure 100% of employees know company policies	
Measurement	*Methodology* Yearly reports	*Frequency* Yearly
Target	• 100 % of employees know and understand all policies.	
Responsible	All employees	

VI. Terms

Personal Data: Any information relating to an identified or identifiable natural person (individual).
Processing: Any operation or set of operation which is performed on personal data or on sets of personal data, whether or not by automated means.
Data Subject: The individual whose personal data is being handled.
Data Controller: Any organization which determines the purposes and means of the processing of personal data.
Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

VII. Aim of the Data Protection Policy

As part of its social responsibility, Thai Ecotrade is committed to international compliance with data protection laws. This Data Protection Policy applies worldwide and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of Thai Ecotrade as an attractive employer.

The Data Protection Policy provides one of the necessary framework conditions for cross-border data transmission among the Group companies. It ensures the adequate level of data protection prescribed by the European Union Data Protection Directive and the national laws for cross-border data transmission, including in countries that do not yet have adequate data protection laws.

VIII. Scope and Amendment of the Data Protection Policy

Thai Ecotrade and its employees are aware that you may wish to be informed about how your personally identifying data and information, such as name, address, telephone/fax numbers or e-mail address etc (“Data”) that you may provide to Thai Ecotrade, are treated. Accordingly, we have developed this policy to explain our use of your Data as well as all our reasonable precautions to keep your Data confidential and secure.
By using our services, you are consenting to the Data collection and use practices described in this policy, as modified from time to time by us. We reserve the right to modify our policy and invite you to consult this policy from time to time in order to familiarize yourself with any changes. The term of this policy are without prejudice to any contractual terms you may enter into with us, which shall prevail over the terms of this policy.

IX. Principles for Processing Personal Data

1. Fairness and Lawfulness

When processing personal data, the individual rights of the data subjects must be protected.
Personal data must be collected and processed in a legal and fair manner.

2. Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

3. Transparency

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

- The identity of the Data Controller
- The purpose of data processing
- Third parties or categories of third parties to whom the data might be transmitted

4. Data reduction and Data economy

Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

5. Deletion

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

6. Factual accuracy; up-to-dateness of data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

7. Confidentiality and Data Security

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

X. Reliability of Data Processing

All data processing is under legal basis with justification for why the controlled processes personal data in a particular way. Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

We do not collect and process data except when voluntarily provided by you. We ensure compliance by our staff with strict standards of security and confidentiality and in processing your data we pledge to fully comply with internationally recognized standards of privacy protection.

1. Customer and Partner Data

1.1 For a contractual relationship

Personal data of the relevant prospects, customers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with.

1.2 For marketing purposes

Customer loyalty or marketing measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. When communicating with the data subject, consent shall be obtained from him/her to process the data for marketing purposes. If the data subject refuses the use of his/her data for marketing purposes, it can no longer be used for these purposes and must be blocked from use for these purposes.

1.3 For Consent

Data can be processed following consent by the data subject. We collect and processes data only for specific and limited purposes. In addition, we may use your data to evaluate the effectiveness of and improve our services to our customers and partners, for our own statistics to evaluate customer interests for improvement, development, and marketing strategies.

The declaration of consent must be obtained in writing or electronically for the purposes of documentation. Any act which is considered to be read or acknowledged for the purposes and do not responded in a timely manner. It is considered as an acceptance and correct use of data for a specific purpose.

1.4 Pursuant to Legal Authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions.

1.5 Pursuant to Legitimate Interest

Personal data can also be processed if it is necessary for a legitimate interest of Thai Ecotrade. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of

the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

1.6 For Highly Sensitive Data

Highly sensitive personal data can be processed only if the law requires this or the data subject has given express consent. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject.

1.7 Automated Individual Decisions

Automated processing of personal data that is used to evaluate certain aspects (e.g. creditworthiness) cannot be the sole basis for decisions that have negative legal consequences or could significantly impair the data subject. The data subject must be informed of the facts and results of automated individual decisions and the possibility to respond. To avoid erroneous decisions, a test and plausibility check must be made by an employee.

2. Employee Data

2.1 For the Employment Relationship

Personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other Group companies.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply. If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

2.2 Pursuant to Legal Authorization

The processing of personal employee data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

2.3 For Consent

Employee data can be processed upon consent of the person concerned. This information can be requested to the extent that is useful to the owner of the data. Declarations of consent must be

submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation.

2.4 Pursuant to Legitimate Interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of Thai Ecotrade. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature.

Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection. Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason.

2.5 For Highly Sensitive Data

Highly sensitive personal data can be processed only under certain conditions. Highly sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject.

Under the company scope of work, highly sensitive data must be keep recorded for the security standard such as criminal background, Drug Screening information, etc. All employee must understand the need and provide the consent for all these records. All these records must be kept in the security place with specific an authorize person to access it only. Employees must understand that these data are collected for use only in situations that are beneficial to the data owner.

2.6 Automated Decisions

If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

2.7 Telecommunication and Internet

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

XI. Data Transfer

Thai Ecotrade is a global company with services customer around the world directly and though our network of certified partners. We may transfer your data to one of its partners, who have agreed to keep your data confidential and secure, outside of your country of residence. The data recipient must be required to use the data only for the defined purposes.

In the event that data is transmitted to a recipient outside Thai Ecotrade and partners to a third country. This country must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation. A legal obligation of this kind can be based on the laws of the domiciliary country of the Group company transmitting the data. In the alternative, the laws of the domiciliary country of the Group company can acknowledge the purpose of data transmission based on the legal obligation of a third country.

We undertake to take all responsible steps to avoid your data to be seen by third parties other than who act for or on behalf of Thai Ecotrade and have agreed to treat your data confidential and secure. Access to data is restricted to those of our employees on a need to know basis and who have been trained to observe strict standards of confidentiality in handing your data.

XII. Rights of the Data Subject

Data Subject has rights to manage and access their personal information in the following rights. Personal Data is to be handled by the responsible manner and cannot do any disadvantage to the data subject.

1. Data Subject has the right to access and update or delete data. We ensure that your data is up to date, accurate and complete. If you would like to access, correct, or delete any data held by us, please do a request in writing to the Data Privacy Officer. We reserve the right to request additional information or documentation to confirm and verify that you are the true data owner.
2. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented. The data subject has right to rectification of your inaccurate data. At the same time an old data was ordered to be edited must be immediately removed from the system.
3. The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
4. If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients. You also have the right to transmit your information to others and in exercising of this right; you shall have the right to such information transmitted directly from us to another where technically feasible. Please note that we will not be responsible for the security once it is transmitted to another party.
5. The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the

interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

XIII. Confidentiality of Processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The “need to know” principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

XIV. Data Protection Control

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. In particular, the responsible department can consult with its Information Security Officer (ISO) and data protection coordinator. The technical and organizational measures for protecting personal data are part of Corporate Information Security management and must be adjusted continuously to the technical developments and organizational changes.

XV. Data Protection Incidents

All employees must inform their supervisor or data protection officer immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (data protection incidents). The management responsible for the function or the unit is required to inform the responsible data protection officer about data protection incidents.

In cases of

» improper transmission of personal data to third parties,
» improper access by third parties to personal data, or
» loss of personal data

the required company reports (Information Security Incident Management) must be made immediately so that any reporting duties under national law can be complied with.

XVI. Responsibilities and Sanctions

The executive bodies of the Group companies are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met. All Management staffs are responsible for ensuring that their function, operation, organizational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection. Compliance with these requirements is the responsibility of the relevant employees.

The relevant management is required to assist the Data Protection Officer with their efforts. The Data Protection Officer can perform checks and must familiarize the employees with the content of the data protection policies.

The departments responsible for business processes and projects must inform the data protection officer in good time about new processing of personal data. For data processing plans that may pose special risks to the individual rights of the data subjects, the Data Protection Officer must be informed before processing begins. This applies in particular to extremely sensitive personal data. The managers must ensure that their employees are sufficiently trained in data protection. Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted in many countries and result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under employment law.

XVII. Data Protection Officer

The Data Protection Officer who works towards the compliance with national and international data protection regulations. The Data Protection Officer is responsible for the Data Protection Policy and supervises its compliance. Any data subject may approach the Data Protection Officer, or the management's staffs, at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

If the management's staffs in question cannot resolve a complaint or remedy a breach of the Policy for data protection, the Data Protection Officer must be consulted immediately. Decisions made by the Data Protection Officer to remedy data protection breaches must be upheld by the management of the company in question.