Title:	**Data Protection Policy**	
Version:	0.4	
Company(ies):	Nippon Sanso (Thailand) Co., Ltd.	
Owner:	Mr. Nobutoshi Hayashi, Compliance Manager;	
Reviewed by:	Mr. Nobutoshi Hayashi, Compliance Manager; & Clara Teo, Regional Chief Compliance Officer	
Reviewed and Approved by:	Mr. Nobutoshi Hayashi, Compliance Manager; Date: Jult 1st,2022	
Reviewed and Approved by: Dr. Suwan Runggeratigul President		Date of Approval/Ratification:
Issued on:	July 15th , 2022	
Effective From:	July 15th , 2022	
President	To be initiated annually by the Compliance Manager & Head of Information Security / IT Manager	

INTRODUCTION AND PURPOSE

1 Nippon Sanso (Thailand) Co.,Ltd. collectively referred to as the "**Company**" gather(s) and use(s) certain Personal Data about individuals. Such information can include customers, suppliers, business contacts, employees and other people the Company has a relationship with or may need to contact.

2 The Company is committed to complying with the Data Protection Law as part of everyday working practices.

3 This Data Protection Policy (this "**Policy**") describes how Personal Data must be collected, handled and stored to meet the Data Protection Law.

4 This Policy ensures that the Company:

4.1 Upholds its commitment to treat Personal Data of employees, customers and stakeholders with the utmost care and confidentiality;

4.2 Protects the privacy rights of employees, customers and stakeholders;

4.3 Is transparent about how it stores and processes individuals' data;

4.4 Protects itself from the risks of data breach.

SCOPE

This Policy applies to:

1. All full-time, part-time, permanent and temporary employees (including freelance workers, contract staff, interns and staff seconded from affiliated companies to the Company), management members and directors of the Company and its subsidiaries. For the purpose of this Policy, a reference to an employee means any of the aforementioned persons; and

contractors, consultants, partners and any other external entity who handle personal data for or on behalf of the Company.

2. The rules in this Policy apply regardless of whether personal information is stored electronically, on paper or on other materials or media.

3. This Policy is not, and should not be confused with, a privacy notice or policy (a statement informing data subjects how their Personal Data is used by the Company).

INFORMATION THE COMPANY COLLECTS

Appendix A sets out the types of Personal Data the Company collects.

DATA PROTECTION LAW

Appendix B sets out the salient points of the data protection legislation in Thailand and guidance published by the data protection authority in Thailand (collectively referred to as the "Data Protection Law").

ORGANISATIONAL SECURITY MEASURES

Responsibilities

1. Everyone who works for or with the Company and who handles Personal Data has responsibility for ensuring Personal Data is collected, stored and handled in line with this Policy and the Data Protection Law.

2. Board of Directors

   The board of directors of the Company is ultimately responsible for ensuring that the Company meets its legal obligations for the protection of data privacy and security.

3. Compliance Representative

   The Compliance Representative, assisted by the Compliance Manager, is responsible for and shall ensure that he/she:

   - Keeps the board updated about data protection responsibilities, risks and issues including data and security breaches;
   - Develops, establishes and reviews all data protection policies and procedures in order to ensure compliance with data protection law;
   - Arranges data protection training for employees at least once a year and for other persons covered by this policy as may be required;
   - Approves any data protection statements or communication together with the legal counsel;

- Handles data protection questions from staff and anyone else covered by this Policy together with the legal counsel
- Checks and approves any contracts or agreements with third parties that may handle the Company's personal data together with the legal counsel;
- Oversees the maintenance of records together with the Head of Information Security or IT Manager.

Data Protection Officer

The Data Protection Officer is responsible for and shall ensure the following (which shall be assumed by the Compliance Manager if no Data Protection Officer had been appointed)

- Act as a liaison between the Company and the regulatory body and is responsible for registration, notification and reporting as required under the Data Protection Law;
- Act as the Company's point of contact for complaints from data subjects;
- Deal with requests from individuals to see the Personal Data the Company holds about them (also called "**data subject access requests**");

Heads of Department

Heads of department are responsible for and shall ensure that:

- All employees within their departments are aware of this Policy and attend data protection training;
- Appropriate processes are implemented within their departments to enable compliance with the Data Protection Law and guidance provided by the Compliance Manager, the Data Protection Officer and the Head of Information Security / IT Manager.

In addition, the head of the human resource department shall ensure that:

- The Company obtains the employee's consent, evidenced by written, electronic or recorded means, to the processing of that employee's personal data related to specified purposes including employment, evaluative and training purposes, and for the purpose of managing or terminating an employment relationship between the Company and the employee (unless the Data Protection Law provides that such consent is not necessary). Where an employee does not give consent or gives partial consent when requested by the Company, the Company may not have the requisite authority to process that employee's Personal Data for the benefit of that employee or disclose that employee's Personal Data a third party pursuant to a request from that

employee. The Company shall ensure that the processing of employees' Personal Data is in accordance with the Data Protection Law.

- The employee signs a confidentiality undertaking which includes an obligation to keep confidential Personal Data learnt during his or her period of employment with the Company and that such obligation shall continue even after the cessation of the employee's employment at the Company for whatever reasons. Where an employee is alleged to have breached such a confidentiality undertaking and such employee disputes such allegation, the head of human resource, and such other independent staff as he or she may designate, shall investigate and report the findings to the Compliance Representative, who will adjudicate on the matter in consultation with such other persons as may be necessary. In countries where business contact information such as business contact's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information is treated as Personal Data under the Data Protection Law, the Company acknowledges that there may be situations where the data subject of such business contact information has made or allowed them to be widely available, in which case different considerations may apply to such business contact information.

Individual Staff

Individual staff, as appropriate for their role and in order to enable the Company to comply with the Data Protection Law, are responsible for and shall ensure that they:

- Complete data protection training;
- Follow relevant advice, guidance and tools/methods provided by the Compliance Representative and Compliance Manager/Data Protection Officer and the Head of Information Security / IT Manager;
- Use Personal Data only for the performance of their duties in the Company and not disclose it unnecessarily or inappropriately, and shall keep confidential Personal Data learnt during his or her period of employment with the Company and such obligation shall continue even after the cessation of the employee's employment at the Company for whatever reasons;
- Report to the Compliance Manager and cooperate with any remedial work arising from personal data breaches;

- Report to the Compliance Manager / Data Protection Officer and cooperate with the fulfilment of data subject access requests;
- Not delete, copy or remove Personal Data when his/her employment ceases with the Company.

Data Privacy Principles

All processing of Personal Data by the Company should observe the following principles:

- Transparency. The Company needs to inform the Data Subject about the nature, purpose and extent of the processing of his or her Personal Data.
- Non-excessive. The processing of Personal Data shall be adequate, relevant, necessary, and not excessive in relation to the purpose.

Data Processing Records

Adequate records of the Company's Personal Data processing activities including the following shall be maintained and shall be kept up-to-date:

- The Data Protection Officer (or the Compliance Manager in the absence of such a position) and the Head of Information Security / IT Manager shall maintain personal data flow mapping of the Personal Data flow within the Company, from the time of collection, including the purpose, description of categories of data subjects, personal data, recipients, and time limits for disposal or erasure of Personal Data;
- A general description of the organizational, physical and technical security measures in place within the Company; and
- The name and contact details of the data protection officer and the Head of Information Security / IT Manager responsible for the protection of Personal Data.

Data Protection Guidance

The head of the department who processes Personal Data is responsible for ensuring that the employees within his/her department and each individual shall comply with policies, procedures and guides as may be issued by the regulatory authority, and the Compliance Manager and/or the Head of Information Security / IT Manager from time to time including the guides set out in or links of which are provided in Appendix C.

The Compliance Manager, with the assistance of the Data Protection Officer and the Head of Information Security / IT Manager, shall review and update such procedures and guides from time to time as necessary.

Data Retention Schedule

Personal Data shall not be retained by the Company for a period longer than necessary. The Compliance Manager and the Head of Information Security / IT Manager shall develop a data retention schedule, and procedures to safeguard the destruction and disposal of such Personal Data in accordance with the Data

Protection Law and local laws and regulations, which shall form part of this Policy in the form of Appendix D.

PHYSICAL SECURITY MEASURES

The head of each department shall ensure limited access to its offices where Personal Data is processed.

The Data Protection Officer or, in the absence of such a position, the Compliance Manager, and the Head of Information Security / IT Manager shall periodically evaluate and readjust the design and layout of the offices spaces and work stations of departments where Personal Data is processed in order to provide privacy to the employees processing Personal Data, taking into consideration the environment and accessibility to unauthorised persons.

TECHNICAL SECURITY MEASURES

The Head of Information Security / IT manager is responsible for developing and evaluating the Company's security measures with respect to the processing of Personal Data and ensuring that such security measures include the following minimum requirements:

- Safeguards to protect the Company's computer network and systems against accidental, unlawful, or unauthorised usage or access, and any interference which will affect data integrity or hinder the functioning or availability of the system;
- The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of the Company's data processing systems and devices;
- Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in the Company's computer network and system, and for taking preventive, corrective, and mitigating actions against security incidents that can lead to a personal data breach;
- A process for regularly testing, assessing, and evaluating the effectiveness of security measures;
- The ability to restore the availability and access to Personal Data in a timely manner in the event of an incident;
- Evaluating any third-party services the Company is considering using to collect, store and/or process data;
- Encryption of Personal Data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

RIGHTS OF DATA SUBJECTS

The Company, and employees who handle Personal Data, shall strictly respect and abide by the rights of the data subjects set out in Appendix B.

DATA BREACHES

In the event of a data breach or sign(s) of a possible data breach, i.e., a breach of the Data Protection Law or of this Policy, or an unauthorised access or retrieval of, or loss of, Personal Information or corporate confidential information, the employee or agent shall immediately report the facts and circumstances to the Compliance Manager, Data Protection Officer and the Head of Information Security / IT Manager within twenty-four (24) hours from his or her discovery for verification as to whether or not notification under the Data Privacy Law is required as well as for the investigation of the reported breach. If required, the Data Protection Officer shall notify the relevant regulatory authority and/or the affected Data Subjects pursuant to requirements and procedures prescribed by the Data Protection Law.

Such investigation shall include the root cause of the breach, the Personal Data possibly involved, recommended measures to be taken by the Company to address the breach and to reduce the harm or negative consequences of the breach.

All data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of Personal Data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the Company.

Reporting

Any Employee with knowledge or suspicion of violation of this Policy must report his/her concerns to the Compliance Manager or to the President/CEO/President Director/General Director/Chairman or through the whistle-blowing system of the Company.

All reports will be treated with the strictest confidentiality.

The Company prohibits retaliation against any Employee for making a good faith report of actual or suspected violations of laws, regulations, or this Policy.

Compliance

The Compliance Manager will provide training on this Policy and on applicable personal data protection laws in general for employees on a regular basis and for such other persons as may be decided by management.

Employees who violate this Policy will be subject to disciplinary action that management considers appropriate.

Questions relating to this Policy should be addressed to the Compliance Manager.

Version History			
Version	**Initiated by:**	**Change Description**	**Date**
1.0	Compliance Manager & Head of Information Security / IT Manager	Baseline version	July 15th, 2022

772

Appendix A

The Company collects the following types of Personal Information:

Types of Personal Data We Collect

Personal data which the Company may collect include but are not limited to :

- personal information such as name, NRIC/FIN/Passport/Social Security number, date of birth, marital status, gender;
- contact information such as postal addresses, email addresses, telephone, mobile phone and fax numbers;
- past and present employment information such as organisation name, organisation type, industry sector, job function and responsibilities, designation, business telephone and fax numbers, business email addresses;
- past and present academic qualifications such as schools attended, courses of study, period of study and academic results;
- professional qualifications and memberships with other professional bodies;
- your billing and payment information, including name of the credit/debit cardholder, credit/debit card number, security code and expiry date;
- medical information, lab results and medical certificates;
- training records;
- details of complaints, disciplinary or criminal records;
- income information;
- photographs;
- photographs, videos and/or audio recordings taken by us or our representatives at our events.

Appendix B

Data Protection Law in Thailand

The following sets out the overview of the data protection provisions which organisations in Thailand are required to comply under the Thailand Personal Data Protection Act, B.E. 2562 (2019) ("PDPA"):

Definitions

"individual" means a natural person, whether living or deceased;

"personal data" means data, whether true or not, about an individual who can be identified —

(*a*) from that data; or

(*b*) from that data and other information to which the organisation has or is likely to have access;

"processing", in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:

(a) recording;

(b) holding;

(c) organisation, adaptation or alteration;

(d) retrieval;

(e) combination;

(f) transmission;

(g) erasure or destruction;

The Company is required to comply with nine main obligations when undertaking activities relating to the collection, use or disclosure of Personal Data. These obligations may be summarised as follows:

Guidelines on the Consent Obligation can be found here:
http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

Appendix C

1. Data Protection Quick Guide

<table>
<tr><td colspan="2">If you handle any information about identifiable people, whether they are employees, employees of our customers or suppliers, visitors or anyone else, you need to be aware that you are dealing with personal data. You must look after all personal data carefully. You must be especially careful with more sensitive information about people, for example concerning their health, sexuality or ethnicity. This Quick Guide is designed to help. Detailed policies, guidance, training and resources are available from the Company's data protection guide as may be published from time to time.</td></tr>
<tr><td>PRINCIPLES AND RIGHTS
Personal data must only be used for the purposes it was provided for, as described at the time of collection. It must be relevant, accurate, treated confidentially/securely, and only retained for as long as it is needed (follow the Company's retention schedule for the disposal or removal of old records). A good rule of thumb is to consider whether someone would be surprised about how you are using their personal data (check the Company's privacy notices to see what they have been told).

Be aware of people's rights: people have a right to know what happens to their personal data and to see copies of it, including emails. They can ask for inaccuracies to be corrected and they can object to how their personal data is being handled, even asking for it to be deleted. Any formal requests you receive should be passed to the Compliance Manager or Data Protection Officer as appropriate.</td><td>SHARING, RISKS AND BREACHES
If you need to share personal data with another organization, even if that organisation just stores personal data for you, you first need to consider the risks of sharing. A written agreement in the correct form may be required. If you are unsure about what to do, speak to your Compliance Manager or Data Protection Officer as appropriate. This is particularly important if the organisation is outside your country.

If you are starting a new project or initiative involving personal data, make sure you consider data protection issues early on.

If you think there has been a leak ("breach") of personal data, make sure you report it as soon as possible, including details of the personal data involved and how widely it may have spread. As the Company may be required to report serious breaches to the regulator, please check with the Compliance Manager or the Data Protection Officer as appropriate. (In the Philippines, registered entities are required to report to the National Privacy Commission within 72 hours upon knowledge of or reasonable belief by the Personal Information Controller or Personal Information Processor that a personal data breach has occurred. In Singapore, organisations are encouraged to notify the Personal Data Protection Commission as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals. A mandatory reporting regime for Singapore entities is expected to be implemented in early 2020.)</td></tr>
</table>

TIPS FOR HANDLING PERSONAL DATA IN THE OFFICE
• **Your office.** If personal data is on your desk or shelves, consider locking your room when you leave it, especially if you are in a publicly accessible building.
 	
• **Your computer.** Use a strong password, change it when needed and don't share it with others. Lock your PC when you leave it unattended and log out at the end of the day. Orient your screen so it can't be viewed by others. Never let others use your computer accounts. Allow IT staff to keep your machine backed-up and updated with the latest security and operating patches. Use passwords/access permissions to protect files and folders on shared drives storing sensitive data. Beware of unsafe websites.
 	
• **Your papers.** Store files and documents about people in locked drawers and cupboards. Know where documents are kept and who has access to them. Ensure confidential waste is shredded or stored securely for collection.
	TIPS FOR HANDLING EMAILS AND PHONE CALLS INVOLVING PERSONAL DATA
	• Emails. Don't copy emails about people wider than you need to. Check email addresses before you send out personal data. Consider sending personal data in a password-protected attachment rather than the body of the email. If you are sending an email to a group of people, especially if it contains anything sensitive, think about using "bcc" so you don't share their addresses. Don't keep emails about people that you or the Company no longer need as these should be deleted in accordance with the Company's retention policies. Be careful when opening emails and attachments from unknown or suspicious sources.
	
	• **Phone calls.** Don't give out personal data about others unless you have verified the caller's identity and you're sure they have a right to have it. Generally, don't supply others' contact details or other personal data to unknown enquirers: take the caller's number and offer to pass messages/queries on. Pass requests from the police and other law enforcement agencies to the Compliance Manager or IT Manager.
	
	• **Out-of-office Notification.** Too much information in your out-of-office notification could pose security risks as such information could be very useful to people performing social-engineering attacks on companies. Don't reveal too much information. Some tips:
	  • Do not list your chain of command in an out-of-office reply and any contact details.
	  • Be intentionally vague. Say you'll be unavailable and that you will be checking your emails.
	  • Leave all personal information and contact details out of your message and signature block.
	  • Rule of thumb is, 'If you wouldn't tell a room full of strangers the information, you shouldn't put it in your out-office-reply.'

TIPS FOR HANDLING PERSONAL DATA	**TIPS FOR WRITING ABOUT PEOPLE**

ON THE MOVE • Your mobile devices. Use a strong password, change it when needed and don't share it with others. Use virtual private networks or secure remote access where possible. Set your devices to lock automatically when not in use. Keep them updated and backed-up. Store them securely. Dispose of old devices carefully. • Portable storage. Avoid using USB sticks to store personal data; if you need to, consider encryption or similar protections against inappropriate access. • Travelling abroad. Consider seeking advice before you travel abroad with mobile devices, and always do so if you are travelling to countries with significant cyber risks.	• **Comments about other people.** Keep comments – whether official or unofficial – fair, appropriate, accurate and justifiable. Always assume that the comment might eventually reach the person it is about.
REMEMBER: You want personal information about yourself to be handled carefully. Always treat other people's information in the same way.	