Personal Data Protection Management System Manual

North East Rubber Public Company Limited

- Mr. Chuwit Jungtanasomboon -

(Mr. Chuwit Jungtanasomboon)

Chief Executive Officer

September 9, 2565

Revision 1

398 Moo 4, Chokchai-Det Udom Road, Khok Ma Sub-district, Prakhon Chai District, Buriram Province 31140

044-666928-29

ner@nerubber.com

www.nerubber.com

Personal Data Protection Management System Manual

North East Rubber Public Company Limited

North East Rubber Public Company Limited was converted into a public limited company on June 8, 2018. It operates in the business of manufacturing smoked rubber sheets, crepe rubber, block rubber, concentrated latex, processing rubber into sheets, and other similar rubber forms. Throughout its past business operations, the company has focused on conducting business efficiently, in line with the business environment and changing global situations in each period.

The company has grown continuously, expanding its production capacity and improving its production processes to deliver quality products to customers both domestically and internationally. To demonstrate its commitment to corporate governance, social responsibility, and environmental responsibility, the company has set a policy for Personal Data Protection. This is to ensure that the collection, use, and disclosure of personal data comply with the Personal Data Protection Act B.E. 2562 (2019) and other related laws, standards, and practices, to properly and securely protect the personal data of data subjects, including employees, customers, business partners, and other relevant individuals.

1. Objectives

Personal Data means "information about a person that enables the identification of that person, whether directly or indirectly, but excludes information of deceased persons specifically" (e.g., name, surname, national ID number, social security number, bank account number, various types of driving licenses, employee performance evaluation data, including copies of these documents). (Sensitive Personal Data includes information such as race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, including facial recognition data, iris scan data, and fingerprint data). ((The company should define the personal data it possesses (Data Mapping) to distinguish genuine personal data from other business-related information that is not personal data protected under personal data protection laws.)) This is to assess the risk of harm that may arise from errors in personal data management and to determine the personal data flow and identify

individuals responsible for managing such personal data.

The company prioritizes the protection of personal data for all employees and related parties, such as customers, partners, contractors, visitors, and contacts, etc., whose data is legally protected. The company has always adhered to this principle. The unauthorized exploitation of personal data or disclosure of identifiable information without consent is a violation of law and company discipline. Therefore, the company has established and implemented this Personal Data Protection Policy within the organization.

North East Rubber Public Company Limited recognizes the importance of personal data protection. Thus, it has developed the Personal Data Protection Policy, which describes how the company handles personal data, including its collection, storage, use, and disclosure, as well as the rights of data subjects. This is to inform data subjects about the company's personal data protection policy. The company hereby announces its Personal Data Protection Policy for everyone's acknowledgment.

The company pledges to protect personal data and establishes necessary measures and guidelines to ensure that personal data collected, used, and disclosed by the company complies with legal requirements.

2. Purpose of the Personal Data Protection Management System

The company has established this Personal Data Protection Management System under the company's Personal Data Protection Policy to serve as a guideline for the company's personal data management, including the collection, use, or disclosure of data. It aims to control internal operations within the company to ensure that the personal data of all individuals is protected in accordance with legal requirements and to serve as a guideline for all employees to ensure that personal data is protected and secured with minimal risk.

3. Applicable Laws

The company has established this Personal Data Protection Management System as a guideline for all employees to define the minimum standards for collection, use, or disclosure, which are subject to the Personal Data Protection Act B.E. 2562 (2019), as well as other related laws, announcements, and regulations.

This Personal Data Protection Management System comprises the Personal Data Protection Policy, the Personal Data Protection Management Manual, and attached documents. In case of any

contradiction or inconsistency between documents, this Personal Data Protection Management Manual shall prevail.

4. Scope of Application

4.1 This Personal Data Protection Management System shall apply to the company, its participants, and company employees.

4.2 This Personal Data Protection covers all data processing, from collection, use, to disclosure of data.

4.3 Personal data protection covers all data subjects, including: Executives/Shareholders, Board of Directors, Partners, Customers, Trade Creditors, Debtors, Government Agencies, Media, Private Organizations, Communities/Society, Employees, Visitors or Website users, Contractors, Consultants, Personal data obtained from outsourced data processing, Contacts, etc.

4.4 In cases where the personal data protection laws of the recipient country have higher standards of personal data protection than those specified in this document, the company shall comply with such laws.

4.5 In cases where there are no personal data protection laws applicable to personal data processing in the recipient country, or if the laws of that country have lower standards than those specified in this document, the company shall comply with the conditions specified in this document.

5. Principles and Guidelines for Personal Data Processing

The company has established principles and guidelines for personal data processing to serve as a framework for employees to follow, ensuring that personal data processing complies with legal requirements.

5.1 Principles of Personal Data Processing

5.1.1 The processing and transfer of personal data must be lawful, clearly defined, and fair.

5.1.2 Personal data processing shall be carried out only for the stated purposes. Any change or addition to the purpose must receive the data subject's consent, unless otherwise required by law.

5.1.3 The company is obligated to inform the data subject of the purpose, the data controller, any transfer or disclosure of data to third parties (if any), and the data subject's rights, prior to or at the time of personal data collection. The company will publish its Personal Data Protection Policy and the Personal Data Protection Management System Manual on the company's website for data subjects and the public to review the guidelines, and will also store them as central company document files.

5.1.4 The company will collect and use personal data only to the extent necessary for the purpose for which the personal data was collected.

5.1.5 Personal data that has exceeded the company's defined retention period, or for which the company no longer has the right or a valid basis to process, will be destroyed by the company.

5.1.6 The company will take reasonable measures to keep personal data accurate, current, and reliable.

5.1.7 The company will establish appropriate security for personal data, covering both management systems and technical aspects, to ensure that personal data is protected as required by law. This includes preventing loss, leakage, unauthorized access, as well as unlawful processing or transfer, and accidental loss.

5.2 Guidelines for Personal Data Processing

The company has established personal data processing guidelines covering the entire process in accordance with the Personal Data Protection Act B.E. 2562 (2019), as follows:

5.1.2 The collection of personal data shall be carried out under a specific purpose and only to the extent necessary within that purpose, or for benefits directly related to the purpose of collection. The data subject must be informed before or at the time of data collection regarding the following details:

1) Purpose of collection

2) Personal data being collected

3) Cases where the data subject must provide personal data to comply with laws or contracts, or to enter into a contract, and must also be informed of the possible consequences of

not providing the personal data.

4) Categories of persons or entities to whom the collected personal data may be disclosed.

5) Rights of the data subject. Data collection must obtain consent from the data subject, unless permitted by law, such as general data that does not require consent (based on contract or legal requirement, e.g., submitting wage payment data to the Revenue Department), or sensitive data that does not require consent (e.g., health data for communicable disease prevention).

5.2.2 Use or Disclosure of Data

The use or disclosure of personal data must be in accordance with the purpose or be necessary for benefits directly related to the purpose of collection, and must obtain consent from the data subject given prior to or at that time, unless otherwise required by law, such as data lawfully disclosed to the public, or to prevent or suppress danger to life, body, or health of a person, etc.

5.3 Practical Methods to Comply with Personal Data Protection Laws

5.3.1 Categorize personal data subjects that the company collects, uses, and discloses clearly. For example:

(a) Personal data subjects who are company personnel, such as executives, employees, temporary workers, etc.

(b) Personal data subjects who are customers, partners, creditors, debtors of the company.

(c) Personal data subjects who are external individuals, such as contacts, visitors, spouses or children of data subjects in group (a) in cases where the company requires information to consider rights under company-defined welfare benefits.

5.3.2 Establish a data flow for personal data obtained, from its acquisition whether directly from the data subject or by other means such as cookies obtained from internet usage data, or by any other method. The company must be able to identify individuals involved with that personal data and limit unnecessary data access. Measures must be in place to prevent unauthorized or unnecessary copying of personal data. A system capable of auditing which relevant personnel have accessed personal data in the company's possession must be maintained.

5.3.3 Assess the risks of personal data in the company's possession to establish a system

for preventing loss, leakage, or theft of data or data storage devices, to efficiently manage particularly sensitive data.

5.3.4 Establish a personal data security system to ensure personal data is secure, accurate, complete, and available, whether in document or electronic form. Access to personal data for use must require user authentication, and only authorized personnel with a legitimate need to use the data as defined by the company shall be granted access.

5.3.5 Define access rights to personal data for relevant company officers.

5.3.6 Define the accountability of company officers who collect, use, or disclose personal data in the event of a personal data breach.

6. Personal Data Protection Management System Framework

1. Setting policies and controls to ensure personal data protection is in accordance with defined standards.
2. Protecting the security of personal data for each category of data subjects.
3. Defining each category of data subjects, which covers the entire processing lifecycle from collection to destruction and the notification of rights.
4. Defining measures for remediation when a personal data breach occurs.
5. Training and developing employees to have knowledge and understanding of personal data protection laws and the Personal Data Protection Management System Manual.
6. Holding meetings to review operations and the Personal Data Protection Management System once a year to ensure efficient control and operation of the personal data management system.

To ensure effective control and operation of the personal data management system, the company has appointed a Personal Data Protection Working Group to oversee and control the Personal Data Protection Management System and to support the implementation of instructions from the company's data controller.

7. Personal Data Protection Criteria

The personal data protection criteria will be defined according to the category of data subjects, controlling the entire processing lifecycle from the initial notification of rights, collection, use or disclosure, to destruction and the exercise of rights. For personal data processing, the

purpose, contact person, and other rights must be communicated to the data subject before or during collection. Consent must be obtained from the data subject, except when consent is not required by law. Disclosure or transfer of data to third parties or overseas must be notified. In case of changes or additions to the purpose, the data subject must be informed, unless otherwise required by law. The criteria include the following elements:

1) Data Collected
2) Source
3) Collection
4) Use
5) Disclosure
6) Transfer
7) Protection
8) Notification of Rights
9) Data Rectification
10) Responsible Party
11) Contact Person and Contact Information

8. Processing Agreements

The company has established guidelines for entering into data processing agreements.

1. Before engaging a data processor, the company must assess the data protection system of the contractor.
2. The contract must specify the purpose, method of data storage, notification to data subjects, use, transfer, disposal of data.
3. The contracting party must sign a personal data protection agreement to comply with the laws or manuals defined by the company.
4. When a data processor is engaged, operations must be controlled to adhere to personal data protection guidelines.
5. Upon expiration of the data retention period, the data processor must be controlled to

destroy the data as specified.

6. The data processor must meet minimum standards and strictly comply with the Personal Data Protection Committee's announcement on the criteria and methods for preparing and maintaining records of personal data processing activities for personal data processors, and must be able to present such records to the company when the company requires access to the information in those records.

9. Rights of the Data Subject

9.1 In cases where the company collects personal data directly from the data subject, the company will inform the individual of the personal data protection policy/information before or during collection, providing at least the following details:

9.1.1 Identity and contact information of the data controller.

9.1.2 Data processor.

9.1.3 Purpose and legal basis for processing in accordance with the data subject's wishes.

9.1.4 Categories of data recipients (if any).

9.1.5 (If any) Facts regarding the data controller's intention to transfer personal data to another country or international organization, as well as an explanation and reference to appropriate safeguards for such transfer.

9.1.6 Period for which personal data will be collected.

9.2 Rights of the data subject to access personal data, request the data controller to rectify personal data, or object to data processing.

9.3 Right of the data subject to withdraw consent at any time.

9.4 Right of the data subject to lodge a complaint with the competent authority.

9.5 The company is obligated to guarantee and protect the following rights of the data subject:

9.5.1 Right to access and obtain a copy of personal data concerning oneself held by the data controller, or to request disclosure of the origin of such personal data for which consent was not given.

9.5.2 Right to receive personal data concerning oneself from the data controller.

9.5.3 Right to object to the collection, use, or disclosure of personal data.

9.5.4 Right to request the data controller to erase or destroy personal data.

9.5.5 Right to request the data controller to restrict the use of personal data.

9.5.6 Right to request the personal data to be accurate, current, complete, and not misleading.

10. Personal Data Protection Measures

The company is obligated to implement appropriate security measures to prevent loss, unauthorized access, use, alteration, modification, or unlawful disclosure of personal data, in accordance with the personal data protection policy established by the company.

11. Auditing

The company has appointed a Personal Data Protection Working Group to review the Personal Data Protection Management System and the company's data controller to audit the company's personal data protection and report to the Chief Executive Officer.

12. Training

12.1 To ensure all employees in the company receive sufficient information, the company will take necessary actions to ensure employees are informed and aware of personal data protection.

12.2 Employees of the company who process personal data must foster an understanding of personal data protection.

13. Document Control

The company is obligated to maintain records of personal data processing activities. The operation of these activities can be in written or electronic form and must be submitted to authorized personnel for review and approval. Details are governed by the document and data control procedures, including retention periods as stipulated by regulations, rules, or laws.

13.1 The record sheet must include the following information:

1) Personal data collected.

2) Purpose of collecting each type of personal data.

3) Information about the personal data controller.

4) Retention period for personal data.

5) Rights and methods of accessing personal data, including conditions for individuals

who have the right to access personal data and conditions for accessing such personal data.

6) Record of use or disclosure of personal data that does not require consent from the data subject.

14. Complaint Process and Related Procedures

14.1 A personal data subject who believes that their personal data has been collected, used, or disclosed in violation of the law or the company's personal data protection policy, and wishes to exercise their rights, can submit a complaint to (the company or the person designated by the company to handle complaints as per Clause 17.2. If a Data Protection Officer is appointed, the personal data subject should complain to the Data Protection Officer) or directly to the Office of the Personal Data Protection Committee, via mail or email.

14.2 Employees of the company who believe that their personal data has been collected, used, or disclosed inappropriately can exercise their rights at (in cases where the company has not appointed a Data Protection Officer, the responsibility for receiving complaints rests with the data controller, which in this case the law defines as a legal entity, thus a complaint can be filed with the company or a person designated by the company to handle complaints).

14.3 The company must respond to the complaint without delay and within 1 month from the date of receiving the complaint.

14.4 In cases where the complainant disagrees with the company's decision, the complainant can appeal to the expert committee appointed by the Personal Data Protection Committee.

15. Liability

The company and/or employees who commit acts in violation of the law are liable for breaching provisions under Sections 77 to 90 of the Personal Data Protection Act B.E. 2562 (2019) and such acts constitute a disciplinary offense of the company.

16. Improvement of the Personal Data Protection Management System

16.1 Data processors and/or employees responsible for the Personal Data Protection Management System can propose improvements or amendments to the manual, requirements, forms, or any other announcements that would enhance the efficiency of the Personal Data

Protection Management System or make it more suitable for the company's operations. Such proposals should be submitted to the Personal Data Protection Working Group for review by the data controller and approval by the Chief Executive Officer.

16.2 The Personal Data Protection Working Group has the authority to consider amending and improving the Personal Data Protection Management System, taking into account its accuracy, appropriateness, adequacy, and efficiency. Whenever an amendment is approved, the approval date must be updated.

16.3 The Personal Data Protection Working Group shall inform all relevant parties of the announcement and ensure compliance with the updates.

17. Responsible Parties and Contact Information

The company has defined responsible parties, their authority, and contact information to ensure that personal data protection is implemented and monitored, and that data subjects' rights are exercised in accordance with the law.

17.1 Responsible Parties and Duties

17.1.1 Personal Data Controller (The Company) has the duty to:

1. Implement appropriate security measures to prevent loss, unauthorized access, use, alteration, modification, or unlawful disclosure of personal data. Such measures must be reviewed when necessary or when technology changes to ensure appropriate security effectiveness, in accordance with the Announcement of the Personal Data Protection Committee on Security Measures for Personal Data Controllers B.E. 2565 (2022) (effective June 21, 2022).
2. In cases where the company, as the data controller, must provide personal data to other parties, such as data processors, the company must take measures to prevent such parties from using or disclosing the data unlawfully or without authorization.
3. Establish a monitoring system to delete or destroy personal data upon expiration of the retention period or when the data is irrelevant or no longer necessary for the purpose of collection, or as requested by the data subject, or when the data subject has withdrawn consent. Exceptions apply if the company has a legitimate need to retain personal data for historical or archival purposes for the public interest, or for research or statistical purposes,

provided appropriate safeguards are in place to protect the rights and freedoms of data subjects as determined by the Personal Data Protection Committee (currently no committee announcement exists), or if it is a duty to exercise state authority granted to the personal data controller, or for the establishment, compliance, or exercise of legal claims, or for the defense of legal claims, or to comply with the law.

4. Notify the Office of the Personal Data Protection Committee of any personal data breaches within 72 hours of becoming aware of it, to the extent practicable, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. If the breach poses a high risk to the rights and freedoms of individuals, the breach must be notified to the data subject along with remedies without delay. Such notification and exceptions shall be in accordance with the announcement specified by the committee.

17.1.2 Data Protection Officer (DPO) has the duty to:

1. Provide advice to personal data processors, including employees involved in compliance with the Personal Data Protection Act and the Personal Data Protection Working Group.
2. Review the operations of involved parties in the collection, use, or disclosure of personal data to ensure compliance with the law.
3. Coordinate and cooperate with the Office of the Personal Data Protection Committee in cases related to the collection, use, or disclosure of personal data by the company's personal data processor.
4. Maintain the confidentiality of personal data known or obtained due to the performance of duties.

17.1.3 Personal Data Protection Working Group has the duty to:

1. Implement instructions from the personal data controller in accordance with the Personal Data Protection Act B.E. 2562 (2019).
2. Screen and provide opinions to management regarding compliance with the Personal Data Protection Act.
3. Monitor progress in implementing the Personal Data Protection Act.
4. Consider and provide recommendations on guidelines and practices for complying with the Personal Data Protection Act.
5. Consider and provide recommendations for improving rules and the Personal Data Protection

Policy to align with laws and various measures.

17.1.4 Data Processor has the duty to:

1. Perform collection, use, or disclosure of data only as instructed by the data controller or according to the operational procedures of each department that has assigned a data processor to record data, and in accordance with the Personal Data Protection Policy only.
2. Implement appropriate security measures to prevent loss, unauthorized access, use, alteration, modification, or unlawful disclosure of personal data as stipulated in the Personal Data Protection Policy, and notify the personal data controller of any personal data breaches that occur.
3. Prepare and maintain records of personal data processing activities in accordance with the established document and data control procedures.

17.1.5 Information Technology Department has the duty to:

1. Perform tasks related to the design, monitoring, review, and recommendation of personal data protection systems.
2. Notify the personal data controller and the Personal Data Protection Working Group of any personal data breaches that occur.
3. Collaborate in resolving loss, leakage, and personal data breaches.

17.2 Designated Contact Person and Contact Channels The company has designated the Data Protection Officer to receive complaints from complainants. Data subjects or complainants can contact the company regarding personal data by notifying the company's Human Resources Department, which will then report to the personal data controller.

Human Resources Department
North East Rubber Public Company Limited
398 Moo 4, Chokchai-Det Udom Road, Khok Ma Sub-district, Prakhon Chai District,
Buriram Province 31140
Telephone: 044-666928-29 Fax: 044-666-212-13
Email: hr@nerubber.com
https://www.nerubber.com