

Lemtech Holdings Co., Limited

Personal Data Protection Management Policy (Translated version)

1. Purpose:

- 1.1. To ensure that the execution of all business activities of the Company complies with the requirements of the Personal Data Protection Act and other relevant laws and regulations.
- 1.2. To articulate the personal data protection objectives that all personnel shall follow; to collect, process, and use personal data within a reasonable scope; to establish the basis for the Company's execution of business operations and management of internal personnel with respect to the use of personal data of customers, suppliers, and employees; to reduce potential legal risks for the Company and its employees; to safeguard customers' rights and interests; and to maintain the Company's reputation.

2. Scope:

2.1. Applicable Objects:

All personnel of the Company, dispatched personnel from manpower dispatch companies, customers or vendors with business dealings with the Company, advisors, and shareholders recorded in the shareholder register are all covered by this policy.

2.2. Protection Scope:

The protection objects of this policy are personal data protected under the Personal Data Protection Act. Relevant regulations are established for the collection, processing, utilization, and international transmission of personal data to ensure the security of personal data.

3. Responsible Units:

3.1. Corporate Governance Unit:

- 3.1.1. Drafting, revision, and management of personal data protection procedures.
- 3.1.2. Promotion and training on personal data protection policy.
- 3.1.3. Maintenance and safekeeping of personal data of directors, managers, and shareholders.

3.2. Human Resources Unit:

- 3.2.1. Establishment, processing, maintenance, and safekeeping of employee personal data.
- 3.2.2. Promotion and training on employee personal data protection policy.
- 3.2.3. Window for complaints, consultations, and incident reporting regarding personal data incidents.
- 3.2.4. Other management planning and execution matters related to personal data protection.

3.3. Information Unit:

- 3.3.1. Establishment of an information security protection network for personal data to prevent risks of hacking, theft, alteration, damage, loss, or leakage of personal data,

and strengthening control of security measures.

3.3.2. Prevention of information security damages and crisis response mechanisms.

4. Risk Assessment:

- 4.1. All personnel of the Company shall comply with this policy. Violation of the Personal Data Protection Act and relevant provisions leading to unlawful collection, processing, utilization of personal data or other infringement of data subjects' rights shall result in disciplinary action in accordance with the Company's relevant regulations and liability for damages.
- 4.2. In cases involving civil compensation, criminal liability, or administrative fines, the Company may terminate the employment relationship and pursue legal liability based on the circumstances.
- 4.3. Employees' obligations regarding the Company's personal data protection shall remain effective even after termination of the employment relationship.

5. Operational Procedures:

- 5.1. The collection, processing, or utilization of personal data (including directors, employees, customers or vendors, and all legal entities and natural persons in the shareholder register) by the Company shall respect the rights of data subjects and be conducted in good faith, without exceeding the specific purpose or the relevant legitimate and reasonable scope.
- 5.2. Methods of obtaining personal data:
 - (1) Employees shall sign the "Company Notice and Consent Form for Collection, Processing, and Utilization of Personal Data" upon employment, under which the Company obtains written consent for collecting, processing, and utilizing general personal data within the specific purpose scope and special personal data within the scope explicitly permitted by law.
 - (2) Consent from data subjects shall be obtained for directors, managers, and shareholder data within the specific purpose scope.
 - (3) For other personal data collection, processing, or utilization, consent from data subjects shall be obtained in accordance with legal requirements based on the nature thereof.
- 5.3. Unless otherwise explicitly permitted by law, personal data concerning medical records, medical treatment, genetics, sex life, health checkups, and criminal records shall not be collected, processed, or utilized.
- 5.4. When collecting personal data directly from data subjects, the following matters shall be clearly informed to them:
 - (1) Name of the collecting entity.
 - (2) Purpose of collection.
 - (3) Categories of personal data.
 - (4) Period, region, targets, and methods of utilization of personal data.
 - (5) Rights exercisable by data subjects and methods under the Personal Data Protection Act and relevant laws and regulations.
 - (6) Impact on data subjects' rights if they freely choose not to provide personal data.

- 5.5. Prior to processing or utilizing personal data not provided by data subjects, the sources of such personal data shall be informed to the data subjects.
- 5.6. If falling under the exemptions from notification under Paragraph 2 of Article 8 and Article 9 of the Personal Data Protection Act, the notification obligations under 5.3 and 5.4 may not be fulfilled.
- 5.7. The Company shall maintain the accuracy of personal data and, upon request from data subjects, respond to inquiries, provide access, make copies, or make corrections/supplements to the collected personal data. In case of violation of the Personal Data Protection Act and relevant laws and regulations in collecting, processing, or utilizing personal data, the Company shall proactively or upon request from data subjects delete, cease collection, processing, or utilization of such personal data.
- 5.8. Unless with written consent from data subjects or necessary for business execution with noted disputes, personal data with any of the following circumstances shall be deleted or cease processing or utilization:
 - (1) Disputes regarding the accuracy of personal data.
 - (2) When the specific purpose of collection disappears or the retention period expires
- 5.9. For personal data not corrected or supplemented due to attributable reasons of the Company, notification shall be given to the parties who were previously provided with such data after correction or supplementation.
- 5.10. In case of theft, leakage, alteration, or other infringement of personal data due to violation of the Personal Data Protection Act or caused by natural disasters, accidents, or other force majeure, upon identification, the Company shall notify the data subjects via telephone, email, mail, fax, or other means sufficient to inform them of the leaked personal data items, impacts produced, and remedial measures taken.
- 5.11. Personal data files held by the Company shall be designated to the information unit for security maintenance to prevent theft, alteration, damage, loss, or leakage of personal data. All employees shall sign the "Employee Confidentiality Agreement," and each custodianship unit shall periodically conduct personal data inventories, recorded in the "Personal Data Inventory Table."
- 5.12. Matters not covered in this policy shall be handled in accordance with the Company's relevant management regulations and laws and regulations of the competent authority.

6. Key Control Focus:

- 6.1. Data subjects shall be informed of the personal data protection policy, and specific purposes for the collection, use, retention, and destruction of personal data shall be identified.
- 6.2. Data subjects' choices and consent regarding the collection, processing, and utilization of their personal data shall be obtained.
- 6.3. The scope of collected and used personal data shall be limited to the specific purposes stated in the notification to data subjects.
- 6.4. Personal data shall be retained only until the specific purpose is fulfilled or the statutory retention period expires, and appropriate measures shall be taken to destroy the personal data.

- 6.5. Disclosure of data subjects' personal data to third parties shall be limited to the specific purpose and with the consent of data subjects.
- 6.6. Physical and logical protection measures shall be implemented for personal data to prevent unauthorized access or use.
- 6.7. In case the Company causes theft, leakage, alteration, or other infringement of personal data, data subjects shall be notified after investigation.

7. Related

Docume

nts:

None.

8. Forms Used:

- 8.1. Company Notice and Consent Form for Collection, Processing, and Utilization of Personal Data.
- 8.2. Employee Confidentiality Agreement.
- 8.3. Personal Data Inventory Table.

This Policy is hereby promulgated on November 13, 2