Walsin Personal Data Protection Management Regulation

Walsin Lihwa Corporation

Article 1 Purpose of Regulation

This regulation (hereinafter "the Regulation") is established in compliance with the Personal Data Protection Act and its enforcement rules, to ensure the effective management of Personal Data protection and maintenance of Personal Data within the Walsin Lihwa Corporation (hereinafter "the Company")

Article 2 Scope of Application

This Regulation applies to all individuals of the Company (including but not limited to controlled subsidiaries, branches, and plants), all processes involving Personal Data, and any companies, vendors, company executives, employees, individuals (including but not limited to dispatched personnel from staffing agencies and temporary workers, as well as their subcontractors) who have business dealings or collaborate with the Company, customers, investors, shareholders, and external entities or individuals who entrust the Company to collect, process, or use Personal Data.

Article 3 Definitions

3.1 Personal Data

Refers to a natural person's name, date of birth, national identification Card number, passport number, physical characteristics, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, sex life, records of physical examination, criminal records, contact information, financial conditions, social activities and any other information that may be used to directly or indirectly identify a natural person

3.2 Sensitive Personal Data

Refers to a natural person's records of physical examination genetics, sex life, healthcare data, and criminal records.

3.3 Personal Data File

Refers to a collection of Personal Data structured to facilitate data retrieval and management by automated or non-automated means.

3.4 Responsible Units

Refers to the Units that collect, process, or use Personal Data as required for business needs and operational execution purposes.

3.5 Collection

Refers to the act of collecting Personal Data in any way.

3.6 Processing

Refers to the act of recording, inputting, storing, compiling/editing, correcting, duplicating, retrieving, deleting, outputting, connecting or internally transferring data for the purpose of establishing or using a Personal Data file.

3.7 Use

Refers to the act of using Personal Data via any methods other than processing.

3.8 Cross-Border Transfer

Refers to the cross-border processing or use of Personal Data.

3.9 Government Agency

Refers to central or local government agencies or administrative entities authorized to exercise public authority.

3.10 Employee Data

Refer to employees' Personal Data collected during employment, including personal submissions and records of job changes, salary adjustments, bonuses, performance evaluations, education and experience updates, attendance, insurance and pension changes, training, announcements, participation in activities, applications, and forms.

3.11 Data Subject

Refers to an individual whose Personal Data is collected, processed or used.

3.12 PDPA

Refers to Personal Data Protection Act.

Article 4 **Responsible Units/Unit**

4.1 Corporate Governance Unit (the "Coordinating Unit")

4.1.1 Responsible for drafting, revising, and managing companywide Personal Data protection policies, related ancillary measures, and implementation guidelines.

4.1.2 Coordinates company-wide Personal Data policy promotion, training, and management planning, including inventory.

4.1.3 Serves as the contact point for complaints, inquiries, and incident reporting related to Personal Data events.

4.1.4 other planning and execution matters concerning Personal Data protection management.

4.2 Human Resources Unit

4.2.1 Responsible for the creation, processing, maintenance, and safekeeping of employee Personal Data.

4.2.2 Acts as the contact point for complaints, inquiries, and incident reporting related to employee Personal Data events.

4.2.3 Assists in executing other management tasks as coordinated by the Coordinating Unit.

4.2.4 Supports the arrangement of Personal Data education and training programs.

4.3 Information Technology Unit

4.3.1 Establishes and maintains an information security protection framework for Personal Data to prevent risks of hacking, alteration, damage, loss, or leakage, and strengthens security control measures.

4.3.2 Implements preventive measures and emergency response mechanisms for information security incidents.

4.3.3 Assists in executing other management tasks as coordinated by the Coordinating Unit.

4.4 Audit Unit

4.4.1 Conducts regular or ad hoc audits of management processes under this Regulation in accordance with internal audit procedures, verifies compliance, provides improvement recommendations, and reports significant deficiencies to the Board of Directors as necessary.

4.4.2 Assists in executing other management tasks as coordinated by the Coordinating Unit

4.4.3 Supports handling of Personal Data incidents and information security crisis response mechanisms.

4.5 Legal Unit

4.5.1 Provides legal consultation and support for incident handling.

4.5.2 Assists in Personal Data education and training programs.

4.6 Each Unit

4.6.1 Implements this Regulation and conducts privacy risk assessments and management for Personal Data obtained and retained by each unit.

4.6.2 Supports handling of Personal Data incidents and information security crisis response mechanisms.

4.6.3 Assists in executing other management tasks as coordinated by the Coordinating Unit.

Article 5 **Personal Data Security Management, Use, and Maintenance**

5.1 All Company units/deparments and personnel shall fully understand and strictly comply with this Regulation and actively participate in the implementation of its management measures.

5.2 The categories of Personal Data obtained, used, and retained by each Unit are listed in **Annex 1**, and the template for the Personal Data Asset Inventory is provided in **Annex 2**.

5.2.1 The Coordinating Unit or its or its designated implementation team may periodically notify units to conduct Personal Data asset inventory.

5.2.2 If there is any change in the categories of Personal Data or data assets retained by a unit, the unit shall immediately update its inventory and submit the revised version to the Coordinating Unit or its designated implementation team for recordkeeping.

5.3 Each unit shall collect, retain, and use Personal Data in compliance with this Regulation.

5.4 Where a unit or responsible personnel needs to collect, process, use, or disclose Personal Data listed in Annex 1 for work or project purposes, the following information must be clearly communicated to the Data Subject prior to implementation:

5.4.1 Company name

5.4.2 Purpose of collection

5.4.3 Categories of Personal Data

5.4.4 Duration, geographic scope, recipients, and methods of use

5.4.5 Data Subject's rights (including access, duplication, supplementation, correction, cessation of collection/use, or deletion)

5.4.6 Impact on the Data Subject's rights if Personal Data is not provided

5.5 If the Data Subject is a director, supervisor, manager, consultant, or designated project participant of the Company (including subsidiaries), the following must also be disclosed:

5.5.1 Name of the business or project

5.5.2 Purpose of collection

5.5.3 Categories of Personal Data

5.5.4 Duration, geographic scope, recipients, and methods of use

Such disclosure shall be made at least by email. If related to job duties or project approvals, the disclosure shall be clearly stated in the approval documents and duly countersigned or approved in accordance with authority requirements.

5.6 Disclosure may be exempt under any of the following circumstances:

5.6.1 Exemption provided by law

5.6.2 Collection is necessary for the Company to fulfill statutory obligations

5.6.3 Disclosure would impede a Government Agency 's lawful duties

5.6.4 Disclosure would harm public interest

5.6.5 The Data Subject is already aware of the required information

5.6.6 Collection is non-commercial and poses no disadvantage to the Data Subject

5.7 For Personal Data collected from sources other than the Data Subject, the source and required disclosure items shall be communicated before processing or use. Such disclosure may be combined with the first use of the data. Exemptions apply under the following conditions:

5.7.1 Circumstances listed in Section 2.6

5.7.2 Data is self-disclosed or otherwise lawfully public

5.7.3 Disclosure to the Data Subject or legal representative is impossible

5.8 The Company shall not collect, process, or use Sensitive Personal Data except under the following conditions:

5.8.1 Explicit legal authorization

5.8.2 Necessary for fulfilling statutory obligations with appropriate security measures

5.8.3 Data is self-disclosed or lawfully public

5.8.4 Necessary to assist the Company in fulfilling statutory obligations with appropriate security measures

5.8.5 Written consent of the Data Subject, provided that such consent does not override legal restrictions or violate the Data Subject's intent

5.8.6 "Written consent" refers to a clear written expression after the Data Subject has been fully informed of the purpose, scope, and impact of consent

5.9 Where the Company engages third parties to collect, process, or use Personal Data, it shall exercise appropriate supervision and clearly stipulate supervisory obligations in the agreement.

5.10 The Company shall respect Data Subject rights and process Personal Data honestly and lawfully, within the scope necessary for the specified purpose, and ensure a legitimate and reasonable connection to the purpose of collection.

5.11 Personal Data shall not be arbitrarily linked across databases or misused.

5.12 Use of Personal Data shall remain within the scope necessary for the specified purpose, except under the following conditions:

5.12.1 Explicit legal authorization

5.12.2 Necessary for public interest

5.12.3 To prevent imminent danger to life, body, liberty, or property

5.12.4 To prevent significant harm to others' rights

5.12.5 For statistical or academic research by public agencies or institutions, provided data is anonymized

5.12.6 Written consent of the Data Subject

5.12.7 Beneficial to the Data Subject

5.13 Any use beyond the specified purpose shall comply with the exceptions under the PDPA and this Regulation and shall be approved by the head of the Responsible Unit, Coordinating Unit, and Legal Unit, with full documentation of the data usage history.

5.14 Correction of Errors or Omissions

Where Personal Data retained by the Company contains errors or omissions, the head of the Responsible Unit shall approve the correction or supplementation, and all related records shall be maintained. If the failure to correct or supplement is attributable to the Company, the Responsible Unit shall, after making the correction or supplementation, notify all parties to whom the data was previously provided or used.

5.15 Accuracy of Personal Data

The Company shall ensure the accuracy of Personal Data and shall proactively correct or supplement such data, or do so upon the request of the data subject.

5.16 Deletion Upon Expiration

When the specific purpose for which Personal Data was collected ceases to exist or the retention period expires, the Responsible Unit shall obtain approval and proceed with deletion and cessation of processing or use. Exceptions apply where continued retention or use is necessary for the performance of duties or business, or where

written consent of the data subject has been obtained or where permitted under applicable law. All deletions or cessations shall be properly recorded.

5.17 Disputed Accuracy

Where the accuracy of Personal Data is disputed, processing or use shall be suspended proactively or upon the request of the data subject. Exceptions apply where processing or use is necessary for the performance of duties or business, or where written consent of the data subject has been obtained, provided that the dispute is noted.

5.18 Unlawful Processing

If Personal Data has been collected, processed, or used in violation of applicable law, the Company shall proactively or upon request delete such data and cease its collection, processing, or use.

5.19 External Disclosure

Personal Data provided externally shall be clearly marked as “Highly Confidential or Strictly Confidential” and include usage restrictions (e.g., “For [specific purpose] only”). Electronic files must be encrypted to ensure secure transmission, and recipients shall be limited to the minimum necessary scope.

5.20 Client Engagement

Where a client has provided written consent in a mandate or engagement letter, the Company may collect, process, and use Personal Data. Upon expiration of the engagement and applicable statutory retention periods, such data shall be deleted or destroyed, except where continued retention or use is necessary for business execution or with written consent of the client.

5.21 Handover Upon Role Change

Personnel responsible for the custody and processing of Personal Data shall, upon any change in position, transfer all storage media and related data files to ensure proper management.

5.22 Deletion Under Statutory Obligation

Where deletion or cessation of collection, processing, or use is required under applicable law or upon request of the data subject, the Responsible Unit shall obtain approval and transfer the matter to the data retention unit for execution. All deletions or cessations shall be properly recorded.

5.23 Disposal of Physical Records

All documents containing Personal Data (including Personal Data forms) shall be properly safeguarded. When discarding paper records, they should first be processed using shredding equipment.

Article 6 Handling Data Subject Rights Requests

6.1 Non-Waiver of Rights

Data subjects shall not waive, nor shall the Company impose contractual restrictions on, the following rights regarding their Personal Data:

6.1.1 The right to inquire or request access.

6.1.2 The right to request copies.

6.1.3 The right to request supplementation or correction.

6.1.4 The right to request cessation of collection, processing, or use.

6.1.5 The right to request deletion.

6.2 Submission Requirements

Requests made under Articles 10 or 11 of the PDPA shall be submitted in writing using the prescribed application form and accompanied by supporting documentation. If the submission is incomplete, the applicant shall be notified to correct deficiencies within a specified period.

6.3 Grounds for Rejection

Applications shall be rejected in writing under any of the following circumstances:

6.3.1 The application remains incomplete after the correction period expires.

6.3.2 Any condition under the proviso of Article 10 of the Act applies.

6.3.3 Any condition under the proviso of Article 11(2) or (3) of the Act applies.

6.3.4 The request is inconsistent with applicable laws or regulations.

6.3.5 The Company shall decide to approve or reject the request within **30 days** of receipt; extensions of up to **30 additional days** may be granted where necessary, with written notice of the reasons for extension provided to the applicant.

6.4 Access and Copies

Data subjects may request the Company to confirm, provide access to, or furnish copies of their Personal Data. The Company shall decide within **15 days** of receipt; extensions of up to **15 additional days** may be granted where necessary, with written notice of the reasons for extension provided to the applicant. The Company may charge reasonable fees to cover necessary costs for providing access or copies.

6.5 Supervised Access

When a Data Subject requests access to their Personal Data, such review shall be conducted in the presence of designated personnel from the relevant Unit and in accordance with the Company's procedures for accessing confidential documents.

6.6 Exceptions to Disclosure

The Company may refuse to provide access or copies under any of the following circumstances:

6.6.1 Disclosure would endanger national security, diplomatic or military secrets, economic interests, or other significant national interests.

6.6.2 Disclosure would impede a Government Agency's lawful duties.

6.6.3 Disclosure would harm significant interests of the Company or a third party.

6.6.4 The nature of the Personal Data file or applicable law prohibits disclosure of its name or contents; restrictions shall follow relevant legal provisions.

Article 7 Personnel Management

7.1 The Company shall, based on business needs, appropriately assign different levels of access rights to various departments and employees (including managerial and non-managerial staff) to control the handling of Personal Data.

7.2 Employees who, in the course of their duties, need to input or output Personal Data shall do so strictly within the authorized scope and access rights granted.

7.3 Employees shall properly safeguard any storage media containing Personal Data and, when performing their duties, collect, process, and use Personal Data in compliance with applicable Personal Data protection laws and regulations.

7.4 Upon termination of employment, employees shall duly hand over all Personal Data in their possession and shall not continue to use such data outside the Company.

7.5 All labor contracts or service agreements entered into between the Company and its employees shall include confidentiality clauses and related penalty provisions to ensure compliance with obligations regarding the confidentiality of Personal Data. The employee's obligation to protect the Company's Personal Data shall remain in effect even after the termination of the employment relationship.

Article 8 Training

8.1. The Company shall conduct regular training sessions on the fundamentals of Personal Data protection laws to ensure employees are aware of and comply with applicable requirements. Records of such training shall be properly maintained.

8.2. The Company's Human Resources Unit shall provide orientation to new employees, explaining the Company's Personal Data protection policies, the scope of responsibilities, and the relevant management measures that must be observed.

Article 9 Personal Data Incident Reporting

9.1 Each Unit of the Company, as required for business operations, may perform tasks involving the input, storage, editing, correction, retrieval, deletion, output, transmission, or other processing of Personal Data and shall be responsible for the management and maintenance of such data. The Information Technology Unit shall implement appropriate security measures, establish internal security control mechanisms, and designate proper storage locations to prevent Personal Data from being stolen, altered, damaged, lost, or disclosed, and shall be subject to periodic audits by the internal audit unit.

9.2 Units and personnel responsible for maintaining Personal Data Files shall adopt appropriate security measures to prevent Personal Data from theft, alteration, damage, loss, or leakage. Each Unit shall establish access rights for Personal Data, implement encryption with appropriate security levels, strengthen access control, and enhance protective measures against unauthorized access such as hacking. Units shall also conduct periodic internal self-assessments and updates.

9.3 In the event of malicious destruction or damage to Personal Data files, operational errors, security incidents, or unauthorized intrusions such as hacking, the relevant Unit shall take immediate emergency response measures and report the Personal

Data security incident (using the Personal Data Breach Notification Form as set forth in Appendix III). Following such notification, the Coordinating Unit shall convene a task force comprising relevant units (such as HR, IT, Legal, Audit, or Media) to investigate the cause, determine responsibility, and take necessary actions based on actual circumstances.

9.4 If Personal Data is stolen, leaked, altered, or otherwise compromised, the Company shall, upon verification, notify the affected data subjects in an appropriate manner and pursue accountability.

9.5 All personnel shall comply with this Regulation. Violations shall be subject to disciplinary action in accordance with the Company's reward and penalty regulations. Where civil liability, criminal responsibility, or administrative penalties are involved, the Company may terminate the employment relationship and, depending on the circumstances, pursue legal action.

9.6 To uphold integrity and protect the rights of Personal Data Subjects, the Company has established a complaint mailbox on its official website to allow data subjects and other stakeholders to raise questions or file complaints. Complaint mailbox: opinion@walsin.com

Article 10 Cross-Border Transfer of Personal Data

10.1 Where the Company transfers Personal Data internationally for business purposes, such transfer may be subject to restrictions imposed by the competent central authority under any of the following circumstances:

10.1.1 The transfer involves matters of significant national interest.

10.1.2 Special provisions exist under international treaties or agreements.

10.1.3 The recipient country lacks adequate Personal Data protection regulations, thereby posing a risk to the rights and interests of the data subject.

10.1.4 The transfer is made indirectly to a third country (or region) in order to circumvent the requirements of applicable law.

10.2 Prior to any international transfer of Personal Data, the Company shall verify whether such transfer is subject to restrictions announced by the relevant competent authority (e.g., the Ministry of Economic Affairs) and shall inform the data subject of the intended destination region for the transfer. The Company shall also supervise the recipient to ensure compliance with the following:

10.2.1 The intended scope, categories, specific purposes, duration, region, recipients, and methods of processing or use of the Personal Data.

10.2.2 Matters relating to the exercise of rights by the data subject as stipulated under Article 3 of the PDPA.

Article 11 Record Retention

All records required under this Regulation, including training records, audit records (including corrective actions), inventory records, and incident reporting records, shall be

retained for a minimum of five (5) years.

Article 12 **Implementation Rules for Subsidiaries and Plant Sites**

Each subsidiary and plant site of the Company may establish detailed implementation rules based on its management and operational needs; however, such rules shall not conflict with this Regulation. In the event of any inconsistency, the provisions of this Regulation shall prevail. Subsidiaries located in other countries or regions (including Mainland China) shall formulate their own Personal Data management regulations in compliance with the applicable laws of such jurisdictions. Nevertheless, the responsibilities and obligations set forth therein shall not be less stringent than those stipulated in this Regulation. Where any provision is less stringent, this Regulation shall take precedence.

Article 13 **Matters Not Covered**

Any matters not addressed in this Regulation shall be governed by the Company's relevant management regulations and applicable laws and regulations issued by competent authorities.

Article 14 **Effective Date and Implementation**

This Regulation shall become effective upon approval by the General Manager and publication by the Company. Any amendments shall follow the same procedure.