

# Personal Data Protection Policy

## Article 1 Purpose

The Phison Electronics Corporation and Subsidiaries Personal Data Protection Policy (hereinafter "the Policy") has been established to strengthen the protection and management of personal data by Phison Electronics Corporation (hereinafter "the Company") and the subsidiaries listed on the Company's business license (hereinafter "subsidiaries"), reduce operational risk, protect the rights of those the information belongs to and ensure compliance.

## Article 2 Scope

The Policy applies to the Company and its subsidiaries. If a subsidiary establishes its own related guidelines because of the size or nature of its business or because of related laws or regulations that it must comply with, it should first submit its proposed plan to the Company's Risk Management Committee for approval.

## Article 3 Objectives

The objectives of protecting and managing personal data are as follows:

1. To comply with laws and regulations on personal data protection, customer contracts and the requirements of related standards and rules;
2. To maintain the legitimate rights and interests of the party of personal data.

## Article 4 Definitions

Personal data: refers to the personal data as defined in the Republic of China Personal Data Protection Act, Enforcement Rules of the Personal Data Protection Act, and relevant industry laws and regulations.

Personal data file: a collection of personal data built to allow information retrieval and management by automatic or non-automatic measures.

Collection: collecting personal data in any form and way.

Processing: to record, input, store, edit, correct, duplicate, retrieve, delete, output, connect or internally transmit information for the purpose of establishing or using a personal data file.

Usage: all methods of personal data use other than processing.

International transmission: The cross-border processing or use of personal data.

Personal data protection management system: the framework and system used to develop, run, oversee, check, maintain and improve personal data protection management.

Personal data infringement cases: using personal data without authorization of the party concerned or illegally collecting, processing and using personal data or otherwise infringing on the rights of the party concerned.

#### **Article 5 Organization and Responsibilities**

The Company appoints the Risk Management Committee (serve as one of the functional committees under the board of directors) as the highest unit to identify and manage privacy/personal data protection risks, and takes the Security and Integration Department as the executive unit. The Company incorporates the operation of the personal data protection management system into the Company's overall operational risk management, and takes appropriate countermeasures.

Dedicated units responsible for collecting, processing, using and keeping personal data shall execute their duties according to provisions in the Personal Data Protection Act.

#### **Article 6 Collect, Process and Use Principles**

1. Any personal data being processed should be identified and the information's scope should be defined;
2. personal data should be collected, processed and used within the necessary scope for specific, lawful purposes and can be updated when necessary to make sure the information remains accurate and complete and see that it remains secure;
3. The parties should be informed of the statutory matters to be notified;
4. The rights that parties can exercise related to their personal data should be respected, including inquiries or requests to review their personal data, requests to make copies of it, requests to supplement or correct it, requests to discontinue the collection, processing or usage of it, and requests to delete it (those rights cannot be waived in advance or restricted by a special agreement);
5. The international transmission of personal data can only be done if it is in compliance with regulations set by the competent authorities and with appropriate protection.
6. When personal data is being used based on exceptions allowed under the Personal Data Protection Act, the usage of the information must be legitimate and legal;
7. A personal data protection management system should be devised and in place to carry out the personal data protection policy; the responsibilities and obligations of employees involved in the operations of the personal data protection management system should be clearly defined;
8. When there is an infringement of an individual's personal data, the case should be handled and reported as quickly as possible based on the "Personal Data Protection Act" and the personal data security and personal data incident handling process of the

Company's "Personal Data Protection Regulations".

### **Article 7 The Operation**

Those in the company who keep personal data files should adopt security and maintenance measures to prevent personal data from being stolen, altered, damaged, destroyed or leaked. The operational framework of the personal data protection management system is based on the PDCA (plan-do-check-act) cycle and implements information security and "Personal Data Protection Act" provisions in the Company's daily management and operations:

1. Plan: Develop a personal data protection management organizational framework, policy, objectives and related guidelines and procedures, and review and adjust them when appropriate on a regular basis.
2. Do: An in place personal data protection management system that includes taking inventory of processes, analyzing personal data flows, developing a list of personal data files, and conducting information management risk assessments to identify hidden risks and gaps; then, based on the findings, set up or adjust information management rules and control mechanisms.
3. Check: Check how effectively the personal data protection system is being implemented based on personal data protection policies, guidelines, processes and control mechanisms and make suggestions for improvement.
4. Act: Based on the review's findings and suggestions, carry out corrective and preventive measures that will continue to improve the personal data protection management system.
5. The company's personal data management unit or personnel must submit an annual self-assessment report to keep management up to date on the security and maintenance of personal data .
6. The Risk Management Committee approves the self-assessment report, and it is kept as part of the company's records.

### **Article 8 Internal Advocacy, Establishment of a System for Rewards, Penalties, Complaints, and Related Disciplinary Measures.**

The Company regularly urges employees to complete education and training related to privacy and personal data protection, so as to enhance staff's vigilance and law-abiding awareness.

The Company conducts risk assessment and control operations on this policy every year. In the event that Phison personnel's breach of the protection of privacy and personal data has been discovered after investigations, we will review and improve the said matter immediately, and take subsequent measures corresponded to our internal

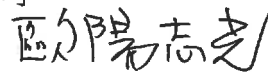
disciplinary policies and procedures. Stakeholders may contact Security and Integration Department of Phison according to the contact mailbox stated in the privacy policy on the official website.

**Article 9 Additional Provisions**

Matters not covered in the Policy should be handled based on regulations set by regulatory agencies and the company's related rules.

群聯電子股份有限公司

總經理 歐陽志光



Phison Electronics Corp. President