

*TAYOPACK Inspired by Zealous*

# **DATA PROTECTION POLICY**



Effective Date: July 2025  
Latest Amendment: March 2026

# TAYOPACK SDN BHD

## DATA PROTECTION POLICY

---

### 1. Introduction

Tayopack Sdn Bhd (“the Company”) is committed to protecting all personal data, customer information, artwork, designs, and confidential business information.

The Company understands the importance of data protection and confidentiality in maintaining customer trust, business integrity, and legal compliance.

This policy explains how personal data and confidential information must be collected, used, stored, protected, and disposed of properly by all employees and related parties.

---

### 2. Scope

This policy applies to all:

- Directors and Management
- Employees (permanent, contract, temporary, interns, and trainees)
- Contractors and service providers
- Suppliers and business partners
- Any third party acting on behalf of the Company

This policy covers all Company and customer information in both physical and electronic form, including:

- Employee and payroll records
  - Emails and databases
  - Customer artwork and design files
  - Product specifications and technical documents
  - Quotations and pricing information
  - CCTV footage
  - Printed and digital confidential documents
-

### **3. Definition**

#### **3.1 Personal Data**

Personal data refers to any information that can identify an individual directly or indirectly.

Examples include:

- Name
  - IC or passport number
  - Contact number
  - Home address
  - Email address
  - Bank account details
  - Employment records
- 

#### **3.2 Confidential Business Information**

Confidential business information refers to any non-public information belonging to the Company or its customers.

This includes:

- Customer artwork and packaging designs
  - Technical drawings and specifications
  - Samples and product information
  - Pricing and quotations
  - Business plans and operational information
  - Company documents and internal records
- 

### **4. Policy Statement**

Tayopack is committed to ensuring that all personal data and confidential information are handled responsibly, securely, and only for authorized business purposes.

The Company strictly prohibits any unauthorized access, sharing, copying, misuse, disclosure, or loss of Company and customer information.

All employees and related parties are responsible for protecting the confidentiality and security of the information they handle during their work.

## **5. Data Protection Principles**

### **5.1 Collection and Use of Data**

Personal data shall only be collected for legitimate business, operational, legal, or employment purposes.

Only necessary information shall be collected and used appropriately.

The Company shall not use personal data for purposes unrelated to business operations without proper authorization.

---

### **5.2 Confidentiality and Access Control**

Access to personal data and confidential information shall only be given to authorized personnel on a need-to-know basis.

Employees must maintain confidentiality of all Company and customer information at all times, including after resignation or termination of employment.

Confidential documents and files must not be left unattended or shared with unauthorized persons.

---

### **5.3 Data Security and System Protection**

The Company shall implement appropriate security measures to protect all information and systems from unauthorized access, misuse, loss, or cyber threats.

Security measures include:

- Password protection for systems, emails, and devices
- Restricted access to confidential files and folders
- Secure storage for physical and electronic documents
- Antivirus and cybersecurity protection
- Proper disposal of confidential documents
- Monitoring and control of system access

Employees are strictly prohibited from:

- Sharing passwords or login credentials
- Allowing unauthorized persons to access Company systems
- Installing unauthorized software or applications
- Using Company systems for unauthorized purposes

To strengthen cybersecurity protection, Company email passwords must be changed every six (6) months or whenever required by Management.

---

## **5.4 Protection of Customer Artwork and Business Information**

Customer artwork, packaging designs, product specifications, samples, technical drawings, and related business information are strictly confidential and must be protected at all times.

Employees and third parties are strictly prohibited from:

- Sharing customer information with unauthorized persons or external parties
- Copying, transferring, or distributing artwork or design files without approval
- Using customer information for personal purposes
- Taking photographs, screenshots, or reproducing confidential documents without authorization

The Company shall implement appropriate safeguards to protect customer information and intellectual property rights.

Any misuse or unauthorized disclosure of customer information may result in disciplinary action, termination of employment, and legal action if necessary.

---

## **5.5 Retention and Disposal of Information**

Personal data and confidential information shall only be retained for as long as necessary for business, operational, or legal purposes.

When the information is no longer required, it must be securely deleted, destroyed, or disposed of properly to prevent unauthorized access or leakage.

---

## **5.6 Employee Responsibility and Awareness**

All employees are responsible for protecting Company and customer information accessed during the course of their duties.

Employees who are issued with Company laptops, desktops, email accounts, or electronic devices must comply with all Company data protection and cybersecurity requirements.

Employees may also be required to sign an Employee Acknowledgement and Confidentiality Agreement before receiving Company devices or access to Company systems.

The Company may conduct awareness sessions or training programs from time to time to strengthen employee understanding of data protection and cybersecurity practices.

---

## **5.7 Incident Reporting and Breach Management**

Any suspected or actual data breach, information leakage, unauthorized disclosure, loss of documents, or cybersecurity incident must be reported immediately to Management or the responsible person in charge.

The Company shall investigate the incident and take appropriate corrective and preventive actions to minimize risks and prevent recurrence.

---

## **6. Management Commitment**

Management is fully committed to protecting personal data, customer information, confidential business information, and Company intellectual property.

The Company will continuously improve its data protection and cybersecurity practices to maintain customer confidence, legal compliance, and business integrity.

---

## **7. Reference**

- Personal Data Protection Act 2010 (PDPA)
- Employee Handbook
- IT Security Policy
- Employee Acknowledgement & Confidentiality Agreement