PUBLIC PACKAGES HOLDINGS BERHAD
PERSONAL DATA PROTECTION POLICY

PURPOSE

Public Packages Holdings Berhad and its subsidiary ("The Group") are committed to ensuring full compliance with the Personal Data Protection Act 2010 of Malaysia ("PDPA"). This Policy outlines the principles, policies and practices adopted by the Group to safeguard personal data and ensure compliance with the PDPA.

REFERENCE

a) Applicable Law: -
Personal Data Protection Act 2010 and its subsidiary regulations.

b) Key compliance requirements: -
(i) Establish and implement internal policies and practices to ensure PDPA compliance;
(ii) Establish a process to manage complaints related to personal data handling;
(iii) Effectively communicate this Policy to all employees;
(iv) Make this Policy and the complaint handling process available upon request; and
(v) Appoint one or more Data Protection officers ("DPOs") and publish the business contact information of at least one DPO for public reference.

DOCUMENTATIONS

The following documents are maintained to support compliance and awareness: -
- ✓ PDPA Consent, Acknowledgement, and Third-Party Data Protection Agreement
- ✓ General PDPA & Cybersecurity Notice
- ✓ Personal Data Protection Notice - staff

COLLECTION OF PERSONAL DATA AND CONDUCTS

a) **Consent requirement**
Explicit consent must be obtained prior to the collection, use, or disclosure of personal data unless an exception under the PDPA applies.

b) **Exceptions to consent requirement**
The Group may collect, use or disclose personal data without consent in the following circumstances: -
i) To respond to an emergency that threatens the life, health or safety;
ii) Where the data is publicly available;
iii) When clearly in the individual's interest and consent cannot be obtained in a timely manner;
iv) Where required for investigations or legal proceedings;
v) Where necessary for evaluation purposes; or
v) Any other circumstances as permitted under the PDPA.

PURPOSE OF COLLECTION, USE AND/OR DISCLOSURE OF PERSONAL DATA

The Group collects, uses and/or disclosures personal data only for legitimate business ad compliance purposes. Example include, but not limited to:

	Category	Personal Data Collected	Purposes of collection/use/disclosure
(a)	Job applicants	Personal data provided in curriculum vitae (CV) or application forms (e.g. email, telephone number, address, educational background, salary history).	To evaluate applicants and carry out recruitment-related processes.
(b)	Employees	Personal and employment related data, bank account details, salary, tax information and etc.	For employment administration, legal and tax compliance, auditing and reporting to authorities.
(c)	Directors and officers	Personal and financial information.	For statutory compliance, administrative and operational management.

	Category	Personal Data Collected	Purposes of collection/use/disclosure
(d)	Shareholders and investors	Data submitted via proxy forms, dividend instructions, meeting document and CDS account details.	To execute corporate actions, address investor queries and distribute corporate communications.
(e)	Third parties	Data collected through interactions (emails, calls, meetings), CCTV footage and transaction-related data.	For business engagement, risk management, compliance and operational purposes.

Personal data is primarily collected from the individuals. Any collection, use and/or disclosure beyond what is necessary will only occur with consent or as permitted by law.

DATA RETENTION, STORAGE AND DISPOSAL

a) ***Data protection and storage***

i) Physical records must be stored in locked cabinets within restricted access areas.

ii) Digital data must be stored on secure servers or cloud systems managed by IT department.

iii) The Group shall not transfer personal data outside Malaysia unless such transfer is permitted under applicable laws and appropriate safeguards are in place to ensure an adequate level of protection.

b) ***Data Retention***

i) Personal data shall be retained for the duration of the business relationship or as required by law (e.g. for tax, employment, audit, regulatory requirements).

ii) Where no statutory retention periods apply, reasonable retention periods will be determined based on business needs.

iii) Once personal data is no longer required, it will be securely deleted or anonymised unless further retention is required by laws.

Example of retention periods:

Type of Data	Retention Periods
Employee records	7 years after termination
Financial records	7 years after financial year end
Job applicant data	1 year from the date of rejection (unless consent is given for longer retention)
CCTV footage	30 to 90 days (unless required for investigation)
Customer/shareholder records	Duration of relationship + up to 7 years

c) ***Data Disposal***

Data that is no longer required will be disposed of securely to prevent unauthorized access or misuse.

Disposal Methods:

a) *Electronic data*: Secure deletion, data-wiping tools, degaussing or physical destruction of media.

b) *Physical records*: Shredding, incineration, or approved secure vendors.

c) *Third-party vendors*: Must comply with the Group's security and confidentiality requirements.

DATA SECURITY MEASURES

The Group have implemented various data security measures, including but not limited to: -

- ✓ data handling and security controls
- ✓ password management
- ✓ email security
- ✓ backup and recovery procedures
- ✓ network security
- ✓ management of third-party contractors
- ✓ mobile device security

For detailed descriptions, please refer to the **Information Security Policy**.

BREACH MANAGEMENT AND REPORTING

Any suspected or confirmed data breach (e.g., lost laptop, unauthorized access, email leak) must be reported immediately to the DPO.

- ✓ The DPO will investigate and complete a Data Breach Incident Report within 24 hours.
- ✓ Affected data subjects will be notified in writing where required.
- ✓ Appropriate containment and corrective actions will be taken.
- ✓ Repeated non-compliance may result in disciplinary action.

All reports must be sent to: **dpo_pp@pph.com.my**

COMPLAINT HANDLING

The Group maintains a formal process to handle complaints and enquiries relating to personal data.

All complaints will be:

- ✓ Acknowledged within a reasonable timeframe; and
- ✓ Investigated and resolved in a timely and appropriate manner.

Where necessary, the DPO will coordinate with relevant departments to ensure proper resolution and effective communication with the data subject.

ORGANISATIONAL ROLES AND RESPONSIBILITIES

The Group assigns the following responsibilities to ensure compliance with the PDPA: -

Role	Key Responsibilities
Board and Executive	Endorse policy, allocate resources, and provide overall risk governance.
DPO	Serve as main PDPA contact, monitor compliance, advise management, handle requests/complaints, maintain policies, liaise with authorities.
IT Team	Implement and maintain security measures, support breach investigations, assist DPO, ensure proper disposal of electronic records.
Human Resources	Obtain valid employee consent, maintain secure records, ensure proper use of employee data, assist with PDPA training.
All Employees	Comply with this Policy, handle personal data appropriately, report breaches immediately, attend mandatory training.

The contact details of the DPO are available on the Group's official website and/or other appropriate communication channels to facilitate public enquiries and requests.

STAFF TRAINING AND AWARENESS

a) All new hires will be brief on PDPA during onboarding.
b) Refresher training will be conducted annually by the DPO.
c) Department heads must ensure their team members understand and comply to this Policy.

REVIEW

This Policy will be reviewed annually or may be updated as necessary to ensure continued compliance with legal and regulatory requirements.