

Kumpulan Perangsang Selangor Berhad
Policy Reference Number

Document Reference Number	KPS/Policy/Legal/PDPP/V3
Date	26 May 2025
Title	Personal Data Protection Policy
Author	Director, Legal & Compliance (Chief Integrity and Governance Officer)
Owning Department	Legal & Compliance
Version	3
Approval Date	6 August 2018
Review Date	Revision 1: 27 May 2022
	Revision 2: 26 May 2025
Approving Body	Board of Directors



KUMPULAN PERANGSANG SELANGOR BERHAD

(Company Registration No:197501002218/23737-K)

PERSONAL DATA PROTECTION POLICY VERSION 3/2025

APPROVED BY BOARD
26 MAY 2025

This Policy is applicable to Kumpulan Perangsang Selangor Berhad Group of Companies

KUMPULAN PERANGSANG SELANGOR BERHAD
PERSONAL DATA PROTECTION POLICY

TABLE OF CONTENTS

NO.	CONTENTS	PAGE
1.	Introduction	
	a) Background	4
	b) Scope	4
	c) Responsibility	4
	d) Approving Authority	5
	e) Date of Implementation	5
	f) Review of Frequency	5
	g) Reference	5
	h) Definition	6
2.	Objectives	6
3.	Statement of Policy	6
4.	Guiding Principles of Personal Data Protection	6
5.	Collection and Processing of Personal Data	9
6.	Sharing Personal Data with Suppliers	11
7.	Transfer of Personal Data outside of Malaysia	11
8.	Right to Data Portability	11
9.	Data Protection Officer	11
10.	Data Breach Notification	11
11.	Non-Compliance	12
12.	Exceptions	12
13.	Queries or Complaints	12
14.	Appendix 1: Definition	13



1.0 INTRODUCTION

1.1. Background

- 1.1.1 Kumpulan Perangsang Selangor Berhad ("KPS Berhad"/ "Company") and its subsidiaries ("KPS Berhad Group") collect, use and retain Personal Data in respect of commercial transaction. This Personal Data Protection Policy (this "Policy") sets out Personal Data protection practices in accordance with the Personal Data Protection Act 2010 and any subsequent amendments to the Personal Data Protection Act 2010 ("PDPA 2010").
- 1.1.2 The Policy is not intended to provide definitive answers to all questions regarding Personal Data. Rather, it is intended to provide guidance to employees and persons who perform services for or on behalf of KPS Berhad Group concerning the collection, use and retaining of Personal Data in the course of business.
- 1.1.3 All terms used in this Policy have the meaning ascribed to it under the PDPA 2010 unless otherwise defined below.

1.2. Scope

- 1.2.1 This Policy applies to KPS Berhad Group.
- 1.2.2 Specifically, this Policy applies to:
 - (a) all individuals who use, process and retain the Personal Data within and/or on behalf of KPS Berhad Group such as employees (whether contract-based including interns), directors, all persons who establish relations with KPS Berhad Group including but not limited to the Supplier, potential business partners, shareholders, and any other parties related;
 - (b) all locations where KPS Berhad Group operates, even where local regulations do not exist; and
 - (c) all methods of contact, including in person, written, via the internet, direct mail, telephone, telex or facsimile.

1.3. Responsibility

- 1.3.1 The Legal and Compliance Department of KPS Berhad is the owner of this Policy. It has full responsibility in the development and maintenance of this Policy including any reviews, changes, amendments, additions or deletions of any provision of this Policy.



1.4. **Approving Authority**

1.4.1 **KPS Berhad**

The Board of KPS Berhad is the approving authority of this Policy.

1.4.2 **Subsidiary companies**

The subsidiary companies are to adopt this Policy upon approval by its board of directors.

1.5. **Date of Implementation**

1.5.1 This Policy is effective immediately upon approval by the Board of KPS Berhad ("**Board**"). For the subsidiary companies, this Policy is effective immediately upon further approval by their respective board of directors.

1.6. **Review Frequency and Amendments**

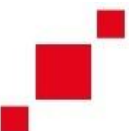
1.6.1 This Policy will be reviewed by Legal and Compliance Department of KPS Berhad every three (3) years at the latest, to ensure the effectiveness of the management and implementation of this Policy.

1.6.2 Any amendments to the Policy shall be approved by the Board except for modifications deemed operational in nature. 'Operational changes' refer to adjustments that do not alter the substantive content of the Policy, such as changes to wording, formatting, or other administrative updates.

1.7. **Reference**

This Policy is issued in conjunction with the laws, by-laws, ordinances, rules, regulations, directives, guidelines, code of conduct issued by the relevant regulatory or statutory bodies including but not limited to:

- (a) Personal Data Protection Act 2010;
- (b) Personal Data Protection (Amendment) Act 2024;
- (c) The Personal Data Protection Guideline on Appointment of Data Protection Officer;
- (d) The Personal Data Protection Guideline on Data Breach Notification;
- (e) Commissioner's Circular No.1/2025 (Appointment of Data Protection Officer);
- (f) Commissioner's Circular No.2/2025 (Data Breach Notification);
- (g) Guide to Prepare Personal Data Protection Notice;
- (h) Employees Handbook;
- (i) Whistleblowing Policy and Guidelines;



- (j) Financial Authority Limit & Delegation of Authority;
- (k) Procurement Policy;
- (l) Compliance Policy;
- (m) Conflict of Interest Policy.
- (n) Cybersecurity Framework; and
- (o) Data Protection Framework.

1.8. Definition

- 1.8.1 The key terms and acronyms appeared in this Policy as defined as per Appendix 1.

2.0 OBJECTIVE

- 2.1. This Policy sets forth:
- 2.1.1 Personal Data protection guidelines and standards that govern KPS Berhad Group in managing the Personal Data that it collects, uses, discloses and retains in commercial transactions.
 - 2.1.2 To ensure compliance with the PDPA 2010.

STATEMENT OF POLICY

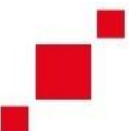
- 2.2. KPS Berhad commits to a high standard of professionalism and ethics in the conduct of our business and professional activities consistent with KPS Berhad's core values of **PRIDE, RESPECT, INTEGRITY, DISCIPLINE AND EXTRA-MILE**. KPS Berhad is committed to the highest standards of openness, integrity, probity and accountability. KPS Berhad aspires to conduct its affairs in an ethical, responsible and transparent manner.

3.0 GUIDING PRINCIPLES OF PERSONAL DATA PROTECTION

- 3.1. The processing of Personal Data shall be in compliance with the seven (7) Personal Data Protection Principles, namely:
- a) the General Principle;
 - b) the Notice and Choice Principle;
 - c) the Disclosure Principle;
 - d) the Security Principle;
 - e) the Retention Principle;
 - f) the Data Integrity Principle; and
 - g) the Access Principle.

i. The General Principle (Section 6 of the PDPA 2010)

KPS Berhad may only process Personal Data with the consent of the Data



Subject whom the Personal Data concerns and/or if the processing of the Personal Data is for the performance of KPS Berhad's duty to which the Data Subject is a party.

ii. The Notice and Choice Principle (Section 7 of the PDPA 2010)

In order to ensure the transparency on the collection and processing of Personal Data, KPS Berhad will need to notify the respective Data Subject before collecting, using or disclosing his/her Personal Data as soon as practical amongst others:

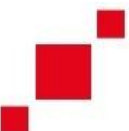
- (a) The processing of his/her Personal Data, by or on behalf of the Data Controller and shall provide the description of the Personal Data to the Data Subject
- (b) The purpose for collection and processing.
- (c) The source of the Personal Data.
- (d) The right of the Data Subject to request for access to and request for correction to be made to the Personal Data and how to contact the Data Controller with any enquiries or complaints in respect of the Personal Data.
- (e) The class of Third Parties to whom Personal Data may be disclosed.
- (f) The choice and means of limiting the processing of the Personal Data including Personal Data relating to other persons who may be identified from that Personal Data.
- (g) Whether it is obligatory or voluntary to supply Personal Data.
- (h) Where it is obligatory for the Data Subject to supply the Personal Data, the consequences to the Data Subject if he/she fails to supply the Personal Data. .
- (i) Privacy Notice is to be in Bahasa Malaysia and English.

iii. The Disclosure Principle (Section 8 of the PDPA 2010)

KPS Berhad requires all employees to be vigilant and exercise reasonable caution when asked to provide any Personal Data to Third Parties. In particular, KPS Berhad must ensure that Personal Data is not disclosed either orally or in writing to any employees without express prior consent of the authorised individual.

However, as and when it is reasonably required, the Personal Data in the possession of KPS Berhad may be only disclosed to the following Third Parties: -

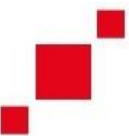
- (a) External professional advisors and auditors; and
- (b) Governmental departments and authorities.



iv. The Security Principle (Section 9 of the PDPA 2010)

KPS Berhad and the employees will ensure that any Personal Data which is collected, stored and processed, is stored securely and practical steps are adopted to ensure the followings:-

- (a) Source documents are well kept. Whereby, the data collected and processed by KPS Berhad and the employees must be stored with the utmost confidentiality and secrecy. A record tracing system should be maintained of files removed and/or returned;
- (b) Paper-based records must not be left where unauthorised employees can gain access to them. The employees should operate a clear desk policy at the end of each working day and when away from the desk or the office for long periods;
- (c) Computerised Personal Data is protected by passwords. If computers are left unattended, the employees must ensure that no personal information may be observed or accessed by unauthorised employees or members of the public. The use of secured screen savers is advised to reduce the chance of casual observation;
- (d) Individual passwords are kept confidential and not disclosed or shared with other employees or Third Parties to enable log-in under any other employees' personal username and password. In exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others;
- (e) The employees must only access service user information on a need-to-know basis and should only view or share data that is relevant or necessary for them to carry out their duties. It is important to ensure that the Personal Data or information is not discussed in inappropriate areas where it is likely to be overheard including conversations and telephone calls. Particular care should be taken in areas where the public have access;
- (f) For Personal Data disclosed to and processed by the external parties such as Supplier, appropriate procedural and technical steps shall be taken to protect Personal Data from accidental or unlawful destruction or accidental loss, alteration or disclosure. These steps include entering into written agreement with the respective parties, which provides sufficient undertaking with regards to PDPA 2010 and to process the Personal Data in accordance with this Policy;
- (g) When physical files or any forms relating to data subject are no longer required, they will be shredded into confetti-like particles



using in-house shredders and bagged or destroyed securely, and the hard drives consisting of those records will be erased off via secure electronic deletion pursuant to the standard operating procedure by the IT and/or Administration Department

- (h) Any employee of KPS Berhad will not process any Personal Data belonging to any Data Subject, whether in soft copy or hard copy, outside of the premises of KPS Berhad unless prior approval is provided by the authorised person.

v. The Retention Principle (Section 10 of the PDPA 2010)

Personal Data obtained should not be retained longer than it is required for its purposes. KPS Berhad has an obligation to ensure that the Personal Data of the Data Subject are destroyed and/or permanently deleted after a specified period of time. All employees are required to refer to the standard operating procedure of the document management should the need to dispose of any Personal Data (including sensitive data) arises. The Company and the employees shall ensure that the Personal Data destroyed are not reconstructed or processed by Third Parties.

vi. The Data Integrity Principle (Section 11 of the PDPA 2010)

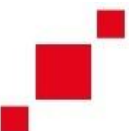
KPS Berhad and the employer must ensure that all Personal Data is accurate, complete, not misleading and kept up-to-date, for which the Personal Data was collected and further processed.

vii. The Access Principle (Section 12 of the PDPA 2010)

Data Subject may request in writing for access to his/her Personal Data held by Data Controller where the Personal Data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under the PDPA 2010. The Data Controller shall respond to the request within thirty (30) days from the receipt of the said request. If the Data Controller is unable to respond within thirty (30) days for whatsoever reason, the Data Controller must inform the Data Subject of the time by which it will respond to the request.

5.0 COLLECTION AND PROCESSING OF PERSONAL DATA

- 5.1. As and when KPS Berhad is required to collect and process Personal Data, KPS Berhad and its employees must abide by the requirements of this Policy and the PDPA 2010. The collection and processing of Personal Data can be in the following circumstances.



5.1.1 ADMINISTRATION AND OPERATION OF KPS BERHAD

KPS Berhad may process Personal Data in order to operate its business, including but not limited to the following:

- (a) Employment context i.e. recruitment purposes, human resources and training staff;
- (b) Billing and taxation purposes;
- (c) Insurance purposes;
- (d) Risk management purposes;
- (e) Internal investigations and audit purposes;
- (f) Information and security purposes, including but not limited to managing and administering e-mail, handling and investigating any security related issues, vulnerability, and/or incidents.
- (g) To maintain records as required and permitted to be collected by law, or other legal purposes (including but not limited to obtaining legal advice and dispute resolution);
- (h) Social investment initiatives purposes organised by KPS Berhad; and
- (i) For all other purposes incidental and associated with any of the above.

Note: This list is not exhaustive and may be extended, varied and amended from time to time.

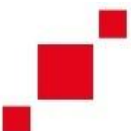
5.1.2 ORGANISATION PROVIDING SERVICES ON BEHALF OF KPS BERHAD SUCH AS SUPPLIERS

KPS Berhad and its employees collect and process Personal Data for various purposes, including the assessment, selection, and administration of potential and existing Supplier.

This also applies when KPS Berhad engages Third Parties to provide services on its behalf, and these services require the collection and processing of Personal Data, KPS Berhad ensures that these Third Parties adhere to the same data protection and confidentiality standards as KPS Berhad.

5.1.3 FROM OR WITH THIRD PARTIES

Personal Data may also be collected and processed by KPS Berhad from or with Third Parties whom it deals or are connected with and from such other sources where they have given consent for the disclosure of Personal Data and/or where otherwise lawfully permitted. Such instances of disclosure of Personal Data with Third Parties to the government authorities and/or authorised Third Parties as required by law.



6.0 SHARING PERSONAL DATA WITH SUPPLIERS

- 6.1. In all cases where Suppliers are granted access to Personal Data, whether the processing of that data is the main purpose of the agreement/contract or incidental to it, the agreement/contract must include reference to the respective parties obligations in compliance to the PDPA 2010.
- 6.2. Personal Data may be shared with Suppliers where this is necessary in relation to the purpose for which the data was obtained, and in line with this Policy.

7.0 TRANSFERS OF PERSONAL DATA OUTSIDE OF MALAYSIA

- 7.1. Personal Data will not be transferred outside KPS Berhad and in particular not a country outside of Malaysia unless: -
 - (a) Consent from the data subject is obtained;
 - (b) If the transfer is necessary for the performance of a contract between the Data Subjects and Data Controller;
 - (c) The transfer is necessary for the performance of a contract between the Data Subject and the Data Controller;
 - (d) The transfer is for purpose of legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; or
 - (e) Any other reasons as allowable under the PDPA 2010.
- 7.2 The employees must seek the clearance of Legal and Compliance Department if they wish to transfer Personal Data outside Malaysia. This is to ensure that the transfer of Personal Data is in compliance with the PDPA 2010.

8.0 RIGHTS TO DATA PORTABILITY

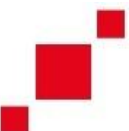
A Data Subject may request for the Data Controller to transmit his/her Personal Data to another Data Controller of his/her choice directly by giving a notice in writing by way of electronic means to the Data Controller, which is subject to technical feasibility and compatibility of data format.

9.0 DATA PROTECTION OFFICER

As and when is required by law, KPS Berhad may mandate the appointment of a Data Protection Officer (DPO) to oversee data protection strategies and ensure compliance.

10.0 DATA BREACH NOTIFICATION

- 10.1 Where a Data Controller has reasons to believe that a Personal Data breach has occurred, the Data Controller shall, as soon as practicable, notify the Commissioner in the manner and form as determined by the Commissioner.
- 10.2 Where the Personal Data breach causes or likely to cause any significant harm to the Data Subject, the Data Controller shall notify the Personal Data breach to the Data Subject in the manner and form as determined by the Commissioner without unnecessary delay.



11.0 NON-COMPLIANCE

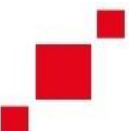
- 11.1 KPS Berhad does not consider any conduct in violation of this Policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties.
- 11.2 Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning consistent with the employee handbook. In addition, KPS Berhad reserves the right to pursue any remedies available, whether civil or criminal and whether at law or in equity, for violations of this Policy.
- 11.3 The employees must immediately report any violations of this Policy to their head of department and/or Legal and Compliance Department.
- 11.4 Accordingly, to the extent permitted by law, KPS Berhad reserves the right not to provide a defence or pay damages assessed against the employees for conduct in violation of this Policy. Individuals who report violations of this Policy in good faith or are involved in the investigation of violations of this Policy will not be subject to reprisal or retaliation, solely as a consequence of such reporting or involvement. Retaliation is a very serious violation of this Policy and should be reported immediately. As for any breach and/or non-compliance by the Third Parties the defaulting parties will be prosecuted in accordance with the PDPA 2010.

12.0 EXCEPTIONS

Any exception from this Policy shall require the approval of the Board unless they are deemed as operational in nature.

13.0 QUERIES OR COMPLAINT

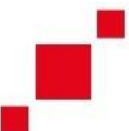
Any questions or concerns about the interpretation or operation of this Policy generally, may be channelled to Legal and Compliance Department via email at legal@kps.com.my.



Appendix 1 : Definition

This list is not exhaustive and full list of definition can be referred in the PDPA 2010 and Personal Data Protection (Amendment) Act 2024

"Collect"	in relation to personal data, means an act by which such personal data enters into or comes under the control of a data controller.
"Commercial Transaction"	means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.
"Commissioner"	means the Personal Data Protection Commissioner appointed under section 47 of PDPA 2010.
"Data Controller"	means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorised the processing of any personal data, but does not include a data processor.
"Data Subject"	means an individual who is subject of the personal data and shall not include a deceased individual.
"Data Processor"	In relation to personal data, means any person other than an employee of the data controller, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes.
"Personal Data"	<p>any information in respect of commercial transactions, which–</p> <ul style="list-style-type: none">(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, <p>that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any</p>



	sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.
"Personal Data Breach"	means any breach of Personal Data, loss of Personal data, misuse of Personal Data or unauthorised access of Personal Data.
"Processing"	in relation to Personal Data, means collecting, recording, holding or storing the Personal Data or carrying out any operation or set of operation on Personal Data, including:- i) The organisation adaptation or alteration of Personal Data; ii) The retrieval, consultation or use of personal data; iii) The disclosure of Personal Data by transmission, transfer, dissemination or otherwise making available; or iv) The alignment, combination, correction, erasure or destruction of Personal Data.
"Sensitive Personal Data"	Means any Personal Data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission of by him of any offence, biometric data or any other personal data as the Minister may determine by order published in the Gazette.
"Supplier"	Suppliers, vendors, consultants, agents, advisors, and goods/service providers of KPS Berhad Group, who have direct dealings with the Group.
"Third Parties"	in relation to personal data, means any person other than– (a) a data subject; (b) a relevant person in relation to a data subject; (c) a data controller; (d) a data processor; or (e) a person authorized in writing by the data controller to process the personal data under the direct control of the data controller.

