



Personal Data Protection Policy

Introduction

Express Power Solutions (M) Berhad and its Group of Companies ("the Group") recognize the importance of protecting personal data entrusted to the Group by customers, employees, suppliers, contractors, business partners, and other stakeholders.

The Group is committed to ensuring that personal data is managed responsibly, securely, and in accordance with applicable personal data protection requirements throughout its business operations, while maintaining the trust of its stakeholders.

Objective

This Group Personal Data Protection Policy ("Policy") establishes the Group's commitment, governance framework, and principles for the responsible management and protection of personal data.

The Policy aims to ensure that personal data is collected, used, disclosed, stored, retained, and disposed of responsibly and in accordance with the Personal Data Protection Act 2010 (Act 709), as amended from time to time, and other applicable personal data protection laws and requirements.

Scope

This Policy applies to Express Power Solutions (M) Berhad and its Group of Companies ("the Group") and covers all personal data collected, processed, stored, disclosed, retained, and disposed of in the course of the Group's business operations.

This Policy applies to all directors, employees, contractors, suppliers, business partners, Data Processors, and other third parties who handle or have access to personal data in connection with the Group's business operations.

Governance and Responsibilities

The Board of Directors and Senior Management provide oversight and direction on personal data protection matters and ensure that appropriate governance, resources, and controls are established to support compliance with applicable requirements.

The designated responsible function, department, or person appointed by the Group, including the Data Protection Officer ("DPO") where applicable, shall coordinate the implementation, monitoring, and continuous improvement of this Policy and related personal data protection activities, with support from relevant functions as appropriate.

All directors, employees, contractors, and relevant third parties who handle personal data are responsible for:

- protecting personal data against unauthorized access, disclosure, alteration, loss, or misuse;
- handling personal data in accordance with this Policy, applicable laws, and approved procedures;
- promptly reporting suspected non-compliance and personal data protection incidents in accordance with applicable procedures; and
- participating in relevant awareness and training activities.



Relationship with Other Group Policies

This Policy shall be read together with other relevant Group policies, procedures, standards, and guidelines. Information security and cybersecurity controls relating to the protection of personal data shall be governed by the Group's Information Security and Cybersecurity Policy and related procedures, while employee personal data, records management, and other operational matters shall be managed in accordance with applicable Group policies and procedures.

Personal Data Protection Principles

The Group shall manage personal data in accordance with applicable personal data protection principles and ensure that personal data is handled responsibly, securely, and transparently throughout its lifecycle.

The Group is committed to the following principles:

a) General Principle

Personal data shall be processed lawfully and for legitimate purposes consistent with the purpose of collection.

b) Notice and Choice Principle

Individuals shall be informed of the collection, processing, use, and disclosure of their personal data.

c) Disclosure Principle

Personal data shall not be disclosed to third parties unless permitted, authorized, necessary for legitimate business purposes, or required under applicable laws.

d) Security Principle

Appropriate measures shall be implemented to protect personal data against unauthorized access, disclosure, alteration, loss, or destruction.

e) Retention Principle

Personal data shall not be retained longer than necessary and shall be securely disposed of when no longer required.

f) Data Integrity Principle

Reasonable steps shall be taken to ensure personal data is accurate, complete, and updated where necessary.

g) Access Principle

Individuals shall be provided with appropriate channels to request access to and correction of their personal data and, where applicable, exercise their right to data portability in accordance with applicable laws and regulations.



Collection, Use, and Disclosure of Personal Data

The Group shall ensure that personal data is collected, processed, used, and disclosed lawfully, fairly, and responsibly in accordance with applicable personal data protection requirements.

a) Collection of Personal Data

The Group shall collect personal data only for legitimate business purposes and where such collection is necessary for the Group's operations, contractual obligations, legal requirements, or other lawful purposes.

The Group shall inform individuals of the purposes for which their personal data is collected and used.

b) Use of Personal Data

Personal data shall only be used for the purposes communicated to individuals or for purposes permitted under applicable laws and regulations.

The Group shall ensure that access to and use of personal data is limited to authorized personnel who require such information to perform their duties and responsibilities.

c) Disclosure of Personal Data

The Group shall not disclose personal data to external parties unless such disclosure is permitted, authorized, necessary for legitimate business purposes, or required by applicable laws, regulations, or contractual obligations.

Where personal data is disclosed to third parties, the Group shall take appropriate measures to ensure that such parties maintain adequate protection and confidentiality of the personal data.

d) Data Processors

Where Data Processors, including suppliers, contractors, service providers, or business partners, process personal data on behalf of the Group, the Group shall implement appropriate contractual, technical, and organizational measures to protect personal data.

e) Cross-Border Transfer

Where personal data is transferred outside Malaysia, the Group shall ensure that such transfers are carried out in accordance with applicable laws, regulatory requirements, and approved Group procedures.

Data Security and Protection Measures

The Group shall implement appropriate technical, organizational, and physical security measures to protect personal data against unauthorized access, use, disclosure, alteration, loss, or destruction.

Data Retention and Disposal

The Group shall retain personal data only for as long as necessary to fulfil the purpose for which it was collected, or as required to comply with applicable legal, regulatory, contractual, and business



requirements. The Group shall establish appropriate retention practices to ensure that personal data is reviewed periodically.

Personal data that is no longer required shall be securely disposed of or anonymized in accordance with approved retention schedules, procedures, and applicable requirements.

The disposal of personal data shall be carried out in a manner that prevents unauthorized access, disclosure, recovery, or misuse of such information.

Relevant functions and departments are responsible for managing, retaining, and disposing of personal data in accordance with this Policy and applicable procedures.

Personal Data Breach Management

The Group is committed to identifying, managing, and responding to any actual or suspected personal data breach in a timely and appropriate manner.

All directors, employees, contractors, and relevant third parties shall promptly report any suspected or actual loss, unauthorized access, disclosure, alteration, or misuse of personal data to the designated responsible function or department.

The Group shall establish and maintain appropriate processes to assess, respond to, and address personal data breaches to reduce potential risks and prevent recurrence.

Where required under applicable laws, regulations, or regulatory requirements, the Group shall notify the relevant regulatory authorities and affected individuals within the applicable timeframe.

The Group shall maintain appropriate records of personal data breaches and implement corrective and preventive measures arising from incident reviews.

Detailed breach reporting requirements, investigation processes, and response actions shall be governed by the Group's applicable procedures and guidelines.

Individual Rights and Requests

The Group recognizes the rights of individuals regarding their personal data and is committed to handling personal data requests in accordance with applicable personal data protection requirements.

Individuals may request access to their personal data held by the Group, request correction of personal data that is inaccurate, incomplete, or outdated, and, where applicable, exercise their right to data portability, subject to applicable laws and regulations.

The Group shall provide appropriate channels for individuals to submit enquiries or requests relating to their personal data and shall ensure that such requests are handled in a fair, transparent, and timely manner.

The Group shall take reasonable steps to verify the identity of individuals making requests and shall assess requests in accordance with applicable legal requirements and the Group's established procedures.

Where requests for access, correction, or data portability cannot be fulfilled, the Group shall provide appropriate explanations where required by applicable laws and regulations.



Detailed requirements relating to the submission, verification, assessment, and processing of personal data requests shall be governed by the Group's supporting procedures and guidelines.

Training and Awareness

The Group shall provide appropriate personal data protection training and awareness activities to directors, employees, contractors, and relevant third parties who handle personal data.

Training and awareness activities shall cover responsible handling of personal data, confidentiality obligations, security practices, incident reporting, and applicable personal data protection requirements.

Personnel are responsible for applying the knowledge gained and complying with this Policy and related procedures.

Monitoring and Compliance

The Group shall monitor compliance with this Policy and relevant personal data protection requirements. Where non-compliance, weaknesses, or gaps are identified, appropriate corrective and preventive measures shall be implemented and monitored.

Policy Approval and Review

This Policy shall be reviewed periodically and whenever significant changes occur to the Group's business operations, technology environment, personal data protection requirements, legal or regulatory requirements, or applicable industry standards.

This Policy was adopted by the Board of Directors on 19 Aug 2026.