Updated: 1st MAY 2026

MARINE & GENERAL
BERHAD

PERSONAL DATA PROTECTION POLICY

PERSONAL DATA PROTECTION POLICY

Marine & General Berhad ("M&G" or "the Company" or "data controller") is committed to protecting the privacy and security of personal data in accordance with the Personal Data Protection Act 2010 (PDPA) and the PDPA (Amendment) Act 2024.

This Policy applies to M&G in its capacity as a data controller and does not override statutory obligations imposed on other entities within the Group.

This Policy explains how M&G collects, uses, disclose, stores, secures, retains and manages personal data. M&G may make changes to this Policy from time to time and will notify any changes via M&G's website.

1. Scope of Policy

The policy is established in accordance with Section 5 (Personal Data Protection Principles) of the PDPA, which requires organisations to comply with the PDPA when processing personal data. This policy applies to all individuals whose personal data is processed by M&G, including:

- Employees, directors, interns, trainees
- Customers, business partners and clients
- Vendors, suppliers, contractors and service providers
- Job applicants and any other individual whose data is collected, stored or processed by M&G

2. Type of Personal Data Collected

This section is guided by **Section 4 of the PDPA (Interpretation)**, which defines personal data and sensitive personal data which may be collected, stored or processed by M&G.

2.1. Personal Data

Information that identifies an individual, directly or indirectly, including:

- Full name, NRIC or passport number
- Contact details: phone, email address
- Financial and banking information
- Date of birth, gender, nationality
- Employment details, education background
- Family/next of kin information
- CCTV recordings, photographs, video footage
- Location/GPS tracking data

2.2. Sensitive Personal Data

Includes data that requires additional protection:

- Physical or mental health information
- Religious beliefs or political opinions
- Race or ethnic origin
- Biometric data (fingerprint, facial recognition, etc.)

3. Source of Personal Data

This section aligns with Section 6 (General Principle) and Section 7 (Notice and Choice Principle) of the PDPA which require that data subjects are informed of how their data is collected and used. M&G collects data from the following sources:

3.1. Customer

M&G collects customer data directly or indirectly when individuals engage with the Company. This includes data obtained through:

- request for services;
- lodge a complaint with us;
- participate in any of our surveys; and/or
- via various means, including online and physical hardcopies at public venues or in any of our premises.

3.2. Vendor, supplier, contractor or service provider

M&G may collect personal information in relation to the individuals who are employed by its vendor, supplier, contractor or service provider (e.g. employee's personal details).

Such personal data may be collected when you, whether as an individual or a corporate entity:

- register as vendor/ supplier/ contractor or service provider with us.
- participate in our tendering process;
- execute or enter into a contract with us;
- request/apply for work permits; and/or
- apply for bunting/banner installations.

via various means, including online and physical hardcopies.

3.3. Job Applicants

M&G will process the data subjects' personal data (including their sensitive personal data such as information about your physical or mental health condition, biometric data, religious belief and criminal conviction, if applicable).

The selection process may involve the supply of further information, and the M&G may obtain such information from third parties (including but not limited to, information from data subjects' referees, public records, background check agencies, recruitment agencies) regarding the qualifications, experience, eligibility and/or other information for recruitment- related purposes. All such information will be kept strictly confidential and used for assessing the data subject's application only.

If data subject's application is unsuccessful, data controller will retain data subjects' personal data for a reasonable period of up to three (3) months for administrative and statistical analysis purposes.

3.4. Employees

M&G may obtain data subject's personal data from them and from a variety of sources, including from third parties connected with the data subjects (e.g. their previous employers, referees, etc), and from other permissible or authorized sources.

3.5. Directors

M&G may obtain the data subjects personal data from them and from a variety of sources, and from other permissible or authorized sources relating to their involvement in the Board of Directors.

Other than personal information obtained from the data subjects directly (as detailed above), M&G may also obtain data subjects personal information from third parties they deal with or are connected with data subjects (including but not limited to credit reference agencies and recruitment agencies), and from such other sources where data subjects have given their consent for the disclosure of information relating to them, and/or where otherwise lawfully permitted.

4. Purposes of collecting and further processing (including disclosing) your personal information

In accordance with Section 6 (General Principle) and Section 7 (Notice and Choice Principle) of the (PDPA), M&G may collect, use, process and disclose personal data for lawful purposes connected with its business and operations, including but not limited to the following ("Purposes"):

a. to manage and administer employment, engagement, or contractual relationships;
b. to provide products or services, manage customer and business relationships, and respond to enquiries or complaints;
c. to conduct due diligence, credit assessments, background checks, and risk management activities;
d. to comply with applicable legal, regulatory, tax, accounting, and reporting obligations;
e. to protect the legitimate interests of the Company, including fraud prevention, security, and dispute resolution;
f. for insurance, audit, corporate governance, and internal control purposes; and
g. for any other purpose reasonably related to the above.

Where required by law, M&G will obtain the consent of the data subject before processing personal data. In other cases, personal data may be processed where such processing is necessary for contractual performance, compliance with legal obligations, or the Company's legitimate business interests, in accordance with applicable law.

5. Disclosure of Personal Information

This section is guided by Section 8 (Disclosure Principle) and Section 9 (Security Principle) of the PDPA, requiring that disclosures are lawful, secure and limited to necessary parties.

M&G may disclose personal data to the following categories of recipients, strictly on a need-to-know basis and for the Purposes stated in this Policy.

a. companies within the M&G Group, subject to appropriate governance arrangements, access controls, and safeguards;
b. third-party service providers, contractors, or professional advisers who process

personal data on behalf of M&G (including but not limited to payroll providers, IT service providers, auditors, insurers, legal advisers, and consultants), who shall be required to comply with applicable data protection obligations;

c. regulatory authorities, law enforcement agencies, or other bodies where disclosure is required or authorised by law; and
d. any other party where disclosure is necessary to protect the legitimate interests of the Company or as otherwise permitted under applicable law.

Where third parties process personal data on behalf of M&G, such parties act as data processors and are contractually required to implement appropriate technical and organisational measures to protect personal data.

6. Accuracy of your Personal Data

As required under Section 11 (Data Integrity Principle) of the PDPA, personal data must be accurate, complete and kept up to date. M&G assumes that all personal data provided by the individual is accurate, complete, not misleading, and up to date, unless M&G is notified otherwise.

7. Storage and Retention of the Personal Information

In accordance with Section 10 (Retention Principle) of the PDPA, personal data shall be stored either in hard copy at the Company's premises or stored in servers operated by the Company or authorised service providers located in or outside Malaysia.

Personal data collected by the Company will be retained only for as long as necessary to fulfil the purposes for which it was collected. Once such purposes have ceased, the personal data will be securely destroyed or anonymised from the Company's records and systems in accordance with proper data disposal practices, unless further retention is required to comply with the Company's operational, legal, regulatory, tax, or accounting obligations.

General Retention Standards:

Accounting & Tax Data

- In accordance with applicable tax laws and corporate record-keeping requirements, including the Income Tax Act 1967, Sales Tax Act 2018, Service Tax Act 2018, and the Companies Act 2016, accounting and tax-related personal data is required to be retained for a minimum period of seven (7) years. Accordingly, M&G retains such accounting and tax-related personal data for at least seven (7) years from the end of the relevant financial year.
- Such records are kept in Malaysia unless otherwise approved by the relevant authority

Employment Data

- In accordance with the Employment Act 1955 and Employment Regulations 1957, employee personal data is required to be retained for a minimum period of six (6) years. Notwithstanding this requirement, M&G has adopted a standardised retention period of seven (7) years for all employee personal data.

- Employee personal data will be securely destroyed by M&G once it is no longer required for employment, statutory, or business purposes, and upon the expiry of the applicable retention period.

Financial Data

- Pursuant to applicable Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) requirements issued by Bank Negara Malaysia, financial-related records are required to be retained for a minimum period of six (6) years following the completion of a transaction or the termination of the business relationship. Notwithstanding this, M&G has adopted a standardised retention period of seven (7) years for financial-related personal data.
- M&G may retain financial-related personal data beyond seven (7) years where:
    - required by law
    - necessary to meet reporting, disclosure, or verification obligations
    - justified by legitimate business or legal grounds; or
    - directed by regulators such as Bank Negara Malaysia or the Securities Commission

Health/Medical Data

- M&G treats health and medical information as sensitive personal data under the PDPA
- Where held by the company (e.g. pre-employment medical check-ups, fitness-for-duty assessments, insurance-related medical records, etc..), retention is guided by applicable healthcare laws and recognised industry practices
- Where applicable, reference is made to the Code of Practice for Private Hospitals in the Healthcare Industry, which provides indicative retention is generally up to seven (7) years, or longer where required by law, limitation periods, or regulatory obligations

8. Right to access and correct personal information

The data subjects have the right to access and correct their personal information held by data controller and the data subjects may request the data controller to correct any of data subjects' personal information that is inaccurate, incomplete or out-of-date, subject to any applicable legal restrictions and contractual conditions.

M&G may impose a reasonable administrative fee, where applicable, to cover the costs involved in processing requests to access or correct personal data. Notwithstanding this, M&G reserves the right to rely on applicable exemptions or exceptions when collecting, using, or disclosing personal data, or when denying access to or correction of personal data, in accordance with applicable laws and regulatory requirements.

If the data subjects have any questions regarding this Policy or wish to request access to or correction of their personal data, or to withdraw their consent for the processing of their personal data for the purposes set out in Section 4 above, such requests may be submitted in writing to the Company. The Company shall appoint a Data Protection Officer ("DPO") under this Policy to oversee and respond to all matters relating to personal data protection.

9. Rights to data portability

Subject to PDPA 2010, as amended by the PDPA (Amendment) Act 2024, M&G may, where applicable and technically feasible, facilitate requests by individuals for the transfer of personal data that they have provided to M&G to another organization, in accordance with applicable legal, regulatory, and operational requirements.

10. Security of Your Personal Data

This section is implemented in accordance with Section 9 (Security Principle) of the PDPA. M&G is committed to protecting personal data against loss, misuse, unauthorised access, disclosure, alteration or destruction.

M&G endeavours, where practicable, to implement appropriate technical, physical, electronic and organisational security measures, in accordance with applicable laws, regulations and industry standards, to safeguard personal data.

Access to personal data is restricted to authorised personnel and service providers who require such access for legitimate business purposes and who are subject to confidentiality obligations.

M&G will review and update its security measures from time to time and ensure the authorised third parties only use the personal data for the Purposes set out in this Privacy Policy.

11. Personal Data from Minors and Other Individuals

This section is implemented in accordance with Section 7 (Notice and Choice Principle) and 8 (Disclosure Principle) of the PDPA, and Section 40(1)(a) of the PDPA, which permits consent to be given by a person legally authorised to act on behalf of the data subject.

Where an individual provides personal data relating to family members, spouse, other dependents or in the case of a corporate entity, personal data of directors, shareholders, employees, representatives, agents and/or other individuals, such individual represents and warrants that the relevant individuals have been informed that their personal data will be provided and processed by M&G and that valid consent has been obtained for the collection, use, disclosure, and transfer of such personal data in accordance with this Privacy Policy.

In respect of minors (i.e. individuals under 18 years of age) or individuals who are not legally competent to give consent, the parent or guardian or person who has parental responsibility over them or the person appointed by court to manage their affairs or that they have appointed to act for them, may provide consent on their behalf to the processing (including disclosure and transfer) of their personal data in accordance with this Privacy Policy.

12. Transfer of Your Personal Data Outside of Malaysia

This section is implemented in accordance with Section 129 (Transfer of personal data to place outside Malaysia) of the PDPA and applicable PDP Guidelines on Cross-Border Transfer of Personal data.

In the course of M&G's operations, personal data may be transferred, stored, or processed in jurisdictions outside Malaysia, including where information technology systems, cloud storage facilities, service providers, group entities, or business partners are located outside Malaysia.

Where personal data is transferred outside Malaysia, M&G will take reasonable steps to ensure that such transfer is carried out in compliance with the PDPA, including by ensuring that appropriate safeguards are in place to protect the confidentiality and security of the personal data, or where the transfer is otherwise permitted under applicable law or regulatory guidance.

Where required by law, M&G will obtain the consent of the data subject prior to transferring personal data outside Malaysia.

13. Data Breach Notification

This section is implemented in accordance with the Personal Data Protection Act 2010 (PDPA) as amended by the PDPA (Amendment) Act 2024, including mandatory personal data breaching notification requirements, and applicable guidelines issued by the Personal Data Protection Commissioner (PDPC).

If a personal data breach occurs, M&G will take immediate action to protect affected personal data and minimise any potential harm. A personal data breach may include loss, theft, unauthorised access, disclosure, alteration, or destruction of personal data.

In the event of a breach:

- Employees, contractors, or service providers must report the incident immediately to the Person In Charge (PIC);
- M&G will investigate, contain, and mitigate the breach as soon as possible;
- Where the breach poses a risk to affected individuals, M&G will notify the PDPC within 72 hours, in accordance with the PDPA (Amendment) Act 2024;
- Affected individuals will be notified where required or appropriate;
- All incidents will be recorded in a Data Breach Register and retained for at least two (2) years.

14. Conflict

In the event of any conflict between the Policy in the English language and the Policy in the Bahasa Malaysia (if issued), the terms in the English language version shall prevail.

15. Changes to Personal Data Protection Policy

The Company reserves the right to change the Policy from time to time without prior notice. The Company advises that you check the latest Policy on our website on regular basis.

16. Data Protection Officer (DPO)

In accordance with Section 12A of the Personal Data Protection Act 2010, as amended by the Personal Data Protection (Amendment) Act 2024, Marine & General Berhad ("M&G") shall appoint at least one Data Protection Officer ("DPO").

The DPO shall be appointed by Management and shall report to Senior Management or the Board, as appropriate, to ensure sufficient independence and authority in carrying out his or her duties.

The appointment of the DPO, including the DPO's business contact information, shall be notified to the Personal Data Protection Commissioner within the statutory timeframe prescribed under the Act. Any subsequent change in the DPO or the DPO's contact information shall likewise be notified within the timeframe required by law.

The DPO shall be responsible for overseeing and monitoring M&G's compliance with the PDPA and any subsidiary legislation, guidelines, or directives issued by the Commissioner.

The DPO's responsibilities include, but are not limited to:

a) Monitoring compliance with this Policy and related internal procedures;
b) Coordinating responses to personal data access and correction requests;
c) Overseeing personal data breach management, including risk assessment and regulatory notification;
d) Acting as the primary point of contact with the Personal Data Protection Commissioner; and
e) Maintaining relevant records, including breach registers and compliance documentation.

The DPO shall be provided with adequate resources, access to relevant information, and authority necessary to perform his or her duties effectively.

Responsibility for compliance with the PDPA remains with the Company as data controller and shall not be delegated solely to the DPO.

17. Policy Governance, Review and Approval

17.1. This Policy may be reviewed and amended from time to time to ensure its continued relevance, alignment with the Company's operational requirements and compliance with applicable laws and regulatory requirements, including the Personal Data Protection Act 2010 as amended.

17.2. Oversight of this Policy shall reside with the Risk Management Committee ("RMC"). Any proposed amendments to this Policy shall be subject to the review and approval of the RMC prior to implementation.

17.3. Notwithstanding the above, the RMC may at any time request for a review of this Policy to address any identified deficiencies, regulatory developments, risk exposures or areas of concern

18. References

- Personal Data Protection Act 2010 [Act 709]
- Personal Data Protection Act 2010 [Act 709]
- Data Residency and Retention Requirements in Malaysia
- Personal Data Protection Guidelines on Cross-Border Transfer of Personal Data (CBPDT)
- AML/CFT Requirements

Updated as of 1st MAY 2026

APPENDIX

DATA BREACH INCIDENT REPORT FORM

Date of Report: _____

CONTACT PERSON

Full Name: _____ Designation: _____

Phone No.: _____ Email: _____

INCIDENT DETAILS

Date of Incident: _____ Time of Incident: _____ ☐ AM ☐ PM

Location:

_____

TYPE OF BREACH (Check all that apply)

☐ Phishing Email or Attempt

☐ Unauthorized Access

☐ Denial of Service (DoS/DDoS) Attack

☐ Lost or Stolen Device

☐ Insider Threat or Suspicious Behavior

☐ Malware/Ransomware Detection

☐ Confidentiality

☐ Compromised Account Credentials

☐ System Misconfiguration

☐ Other: _____

INCIDENT DESCRIPTION

_____

_____

_____

_____

_____

_____

HOW WAS THE INCIDENT DETECTED? (Check all that apply)

☐ Antivirus or Endpoint Detection ☐ Firewall Alert or SIEM System

☐ Reported by Employee/User ☐ External Notification

☐ Routine Audit or Monitoring ☐ Other: _____

ACTIONS TAKEN

Were steps taken to contain or mitigate the incident? ☐ Yes ☐ No

Describe the actions taken:

_____

_____

_____

_____

_____

OFFICE USE ONLY

Reported received by: _____

Position: _____

Signature: _____

Date: _____

OFFICE DISPOSAL FORM

Date of Request: _____

REQUESTOR DETAILS

Name: _____

Department: _____ Position: _____

ITEM DETAILS

Category (Tick One):

☐ Documents / Records ☐ Digital Files / Softcopy Records

☐ Other: _____

Item Description: _____

Asset Tag / Serial No./ File No. (if applicable): _____

Quantity: _____

Condition: ☐ Good ☐ Repairable ☐ Obsolete ☐ Damaged ☐ Beyond Repair

REASON FOR DISPOSAL

☐ Obsolete / Outdated ☐ Duplicate or redundant records ☐ Damaged

☐ Data retention period expired ☐ Other: _____

Detailed explanation (if required): _____

DISPOSAL METHOD

☐ Recycle ☐ Secure Shredding (for documents)

☐ E-Waste Disposal ☐ Other: _____

Vendor / Contractor (if applicable): _____

DATA CONFIRMATION (For IT / Electronic Items)

☐ Data backup completed ☐ Data permanently erased / wiped

☐ Storage media removed and destroyed ☐ Not applicable

Certified by: _____ Signature: _____

Date: _____

APPROVAL

Requested/ Proposed by (Requestor):

Name: _____ Signature: _____

Date: _____

Witness by:

Name: _____ Position: _____

Signature: _____ Date: _____

PERSONAL DATA ACCESS REQUEST / CORRECTION FORM

IMPORTANT NOTES:

- This form is for individuals requesting access to or correction of personal data.
- Please note that Marine & General Berhad (the Company) reserves the right to restrict your access to certain personal data or refuse to comply with your Personal Data Access Request as may be permitted under the Personal Data Protection Act 2010 and Personal Data Protection (Amendment) Act 2024.
- Third Party Requestor is to be present at the relevant office / branch to submit this form and for verification of information and documents required.
- Personal data collected on this form is required to enable your Personal Data Access Request to be processed, and will only be used in connection with such request.
- If you have any queries / need any guidance in filing up this form, you may contact: Personal Data Protection Officer at nazrain@marine-general.com.my

☐ I would like to access my personal data

☐ Correction / update of my personal data

☐ I am making this request on behalf of another person (complete Section 3)

SECTION 2: ABOUT YOURSELF		
Full Name (as per NRIC / Passport)		
NRIC No. / Passport No. *(Please provide a photocopy of your NRIC / Passport)*		
Contact Details	Telephone No.:	
	Fax No.:	
	Email Address:	
	Home Address:	
Please state the nature of your relationship with the Company	☐ A current / former customer ☐ A current / former employee ☐ A current / former vendor / supplier / contractor / distributor / business partner / service provider ☐ Other (specify) _____ ** delete where applicable*	

SECTION 3: THIRD PARTY REQUESTOR'S PARTICULARS	
Full Name (as per NRIC / Passport)	

NRIC No. / Passport No. *(Please provide a photocopy of your NRIC / Passport)*		
Contact Details	Telephone No.:	
	Fax No.:	
	Email Address:	
	Home Address:	
Name of individual (Data Subject)		
NRIC No. / Passport No. of the individual		
Please state the nature of the individual's relationship with the Company	☐ A current / former customer ☐ A current / former employee ☐ A current / former vendor / supplier / contractor / distributor / business partner / service provider ☐ Other (specify) _____ * *delete where applicable*	
Please state the nature of your relationship with the individual	Please tick whether you are the individual's: ☐ Parent ☐ Legal Guardian ☐ Legal Representative appointed by Court ☐ Administrator of the individual's estate ☐ Other (specify) _____	
Please enclose the relevant supporting documents. Please note that the document must be certified by a Commissioner for Oaths, a Notary Public or an Advocate & Solicitor Please also enclose the data subject's NRIC photocopy	☐ Court Order / Power of Attorney ☐ authorisation letter from the individual ☐ Other (specify) _____	
SECTION 4: DETAILS OF THE REQUEST		
A. IF ACCESS REQUEST		
Please describe the personal data requested (be specific, e.g., employment records, account information, etc.)		

Preferred format	☐ View ☐ Email copy ☐ Hard copy by mail ☐ Self Collection
B. IF CORRECTION REQUEST	
Please state the personal data you are requesting to have it corrected or updated	
Correct / updated information	
Supporting documents attached (if any)	
SECTION 5: DECLARATION	
Please sign this form, check the information you have provided, then submit this form together with the relevant supporting documents	By signing this form, I confirm that the information given in this form and any supporting documents enclosed are true and accurate. To the extent that I have provided a third party's personal data, I confirm that I have obtained his consent to disclose his personal data to you. I understand that it will be necessary for the Company to verify my identity and my authorisation (if applicable) and that the Company may contact me for more detailed information in order to locate the personal data requested. I also consent to the Company processing any and / or all personal data provided by me in accordance with the Company's Privacy Policy. Signed : _____ Date : _____
SECTION 6: OFFICIAL USE ONLY	
Received by:	
Name:	
Designation:	
Office / branch:	
Date received:	
Decision:	☐ Approved ☐ Rejected

Grounds for rejection:	☐ Unable to verify identity ☐ Incomplete form / supporting documents ☐ Personal data not in our possession ☐ Others Remarks (if any): _____ _____ _____