

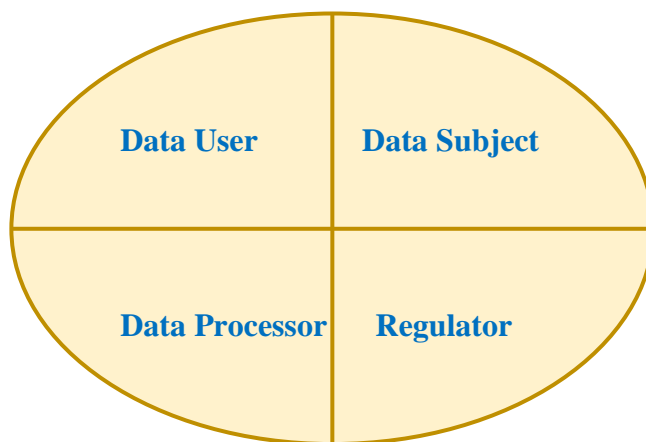
## MEWAH GROUP MALAYSIA PERSONAL DATA PROTECTION POLICY

We, Mewah Group Malaysia Entities<sup>1</sup> (“MGMEs”), are committed to ensuring compliance with the **Personal Data Protection Act 2010** (“Act”). We recognize the importance of personal data to our business and the importance of respecting the privacy rights of individuals. This Data Protection Policy (“**Policy**”) sets out the principles which we will apply to our collection, recording, holding, storing, usage, disclosure (“**process**”) of personal data to comply with the applicable laws and regulations. We will keep confidential all information and documents relating to the processing of personal data.

### A. FRAMEWORK

The Act sets out seven data protection principles which must be followed in relation to the processing of personal data. In order to fully appreciate the requirements of the Act, some important terms of the Act that we should take note of are as follows:

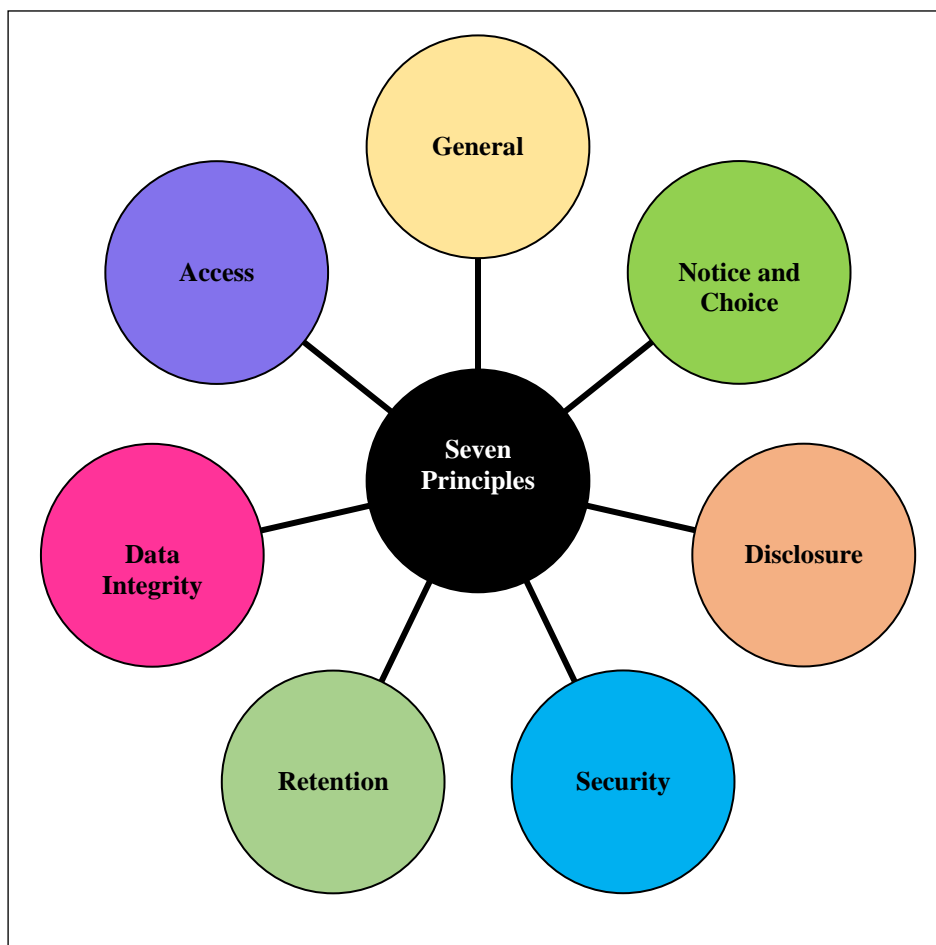
#### Personal Data Protection Act 2010 - Key Parties



Commercial transactions	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	the Personal Data Protection Commissioner appointed under section 47 of the Act.
Correction	in relation to personal data, includes amendment, variation, modification or deletion.
Data processor	any person other than an employee of the data user, who processes the personal data solely on behalf of the data user and does not process the personal data for any of his own purposes.
Data subject	an individual who is the subject of the personal data.
Data user	a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor.

Personal data	<p>any information in respect of commercial transactions which:-</p> <ul style="list-style-type: none"> <li>(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;</li> <li>(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or</li> <li>(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, 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 user, including any 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.</li> </ul>
Processing	collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data including organization, adaptation or alteration, retrieval, consultation or use of, disclosure by transmission, transfer, dissemination or otherwise making available, alignment, combination, correction, erasure or destruction of personal data.
Relevant filing system	any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set of information is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
Sensitive personal data	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 or alleged commission by him of any offence or any other personal data as the Minister may determine.
Third party	any person other than a data subject, a relevant person in relation to a data subject, a data user, a data processor or a person authorized in writing by the data user to process the personal data under the direct control of the data user.
Vital interests	matters relating to life, death or security of a data subject.

## **B. SEVEN PRINCIPLES**



### **Principle I - General Principle**

The General Principle requires the processing of personal data lawfully and in accordance with the purpose for which the personal data is collected.

We shall ensure that personal data is processed only after at least one of the conditions in Section 6(1)(a) or Section 6(2) of the Act is met and in the case of sensitive personal data, at least one of the conditions in Section 40(1) of the Act is also met.

#### **a. Lawful processing**

The conditions pursuant to Section 6(1)(a) and Section 6(2) of the Act are as follows:-

- (1) The data subject has given his consent to the processing.
- (2) The processing is necessary for the performance of a contract to which the data subject is a party.
- (3) The processing is necessary for the taking of steps at the request of the data subject with a view to entering into a contract.
- (4) The processing is necessary for the compliance with any legal obligation to which we are subject to other than an obligation imposed by a contract.

*MGMES Policy version 1.0 – 08.08.2018*

- (5) The processing is necessary to protect the vital interests of the data subject.
- (6) The processing is necessary for the (i) administration of justice or (ii) exercise of any functions conferred on any person by or under any law.

The conditions pursuant to Section 6(1)(a) and Section 6(2) of the Act, for processing of sensitive personal data, are as follows:

- (1) The data subject has given his explicit consent to the processing.
- (2) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on us in connection with employment.
- (3) The processing is necessary (a) in order to protect the vital interests of the data subject or another person, in a case where (i) consent cannot be given by or on behalf of the data subject, or (ii) we cannot reasonably be expected to obtain the consent of the data subject, or (b) in order to protect the vital interest of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
- (4) The processing (a) is necessary for the purposes of or in connection with any legal proceedings, (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- (5) The processing is necessary for the (a) administration of justice, or (b) exercise of any functions conferred on any person by or under any written law.
- (6) The processing is necessary for medical purposes and is undertaken by (a) a health professional or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
- (7) The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

*b. Purpose driven and directly related to our activities*

Processing of personal data must be purpose driven, in that it must only be processed for a lawful purpose directly related to our activities, the processing is necessary for or directly related to that purpose and the personal data is adequate but not excessive in relation to that purpose. Our privacy notices will specify the purposes for which we will process personal data. We shall obtain personal data only for one or more lawful purposes as specified in the respective privacy notices.

To ensure that the personal data is adequate, relevant and not excessive, we:-

- (1) shall identify the personal data needed for a particular purpose and we collect the minimum amount required to properly fulfil that purpose;
- (2) shall not hold personal data on a “just-in-case” basis because we think it might be useful in the future but without having any clear idea of what that future purpose might be;
- (3) shall keep personal data up-to-date (otherwise the personal data which were originally adequate may cease to be so); and
- (4) shall not keep personal data for longer than necessary (otherwise the personal data may cease to be relevant and become excessive).

c. Data subject's consent

The consent of the data subject may be in any form which can be recorded and maintained properly by us.

**Principle II - Notice and Choice Principle**

The Notice and Choice Principle requires us to give the data subject written notice of the processing of his personal data and choices available to him in connection with such processing.

For compliance with Notice and Choice Principle, we achieve this by giving data subjects a privacy notice which meets the following requirements:

a. Content of privacy notice

- (1) The identity of the data user.
- (2) The description of the personal data.
- (3) The purposes for which the personal data is being or is to be processed.
- (4) Any information available to us as to the source of that personal data.
- (5) The data subject's right to request access to and to request correction of his personal data and mode by which he is able to contact us with any enquiries or complaints in respect of his personal data (the designation of the contact person, phone number, fax number, email address and other related information).
- (6) The class of third parties to whom we disclose or may disclose the personal data to.
- (7) The choices and means by which we offer the data subject for limiting the processing of his personal data, including personal data relating to other persons who may be identified from his personal data.
- (8) Whether it is obligatory or voluntary for the data subject to supply the personal data.
- (9) Whether it is obligatory for the data subject to supply the personal data and the consequences should he fail to do so.
- (10) The notice must be in Bahasa Malaysia and the English language and the data subject must be given a clear and readily accessible means to exercise his choice(s) in both languages.

b. Timing of privacy notice

The privacy notice must be given to the data subject at the right time. Where we obtain personal data directly from the data subject, we shall give the privacy notice to the data subject at the time we obtain his personal data.

c. Position and format of privacy notice

- (1) The privacy notice must be reasonably prominent and in reasonably legible font.
- (2) The privacy notice must be included at every point where we collect personal data, such as application forms, websites, call centre scripts etc.
- (3) If, the privacy notice is provided online, it must be strategically placed so that it can be seen and not hidden behind a hypertext link.

### ***Principle III - Disclosure Principle***

This Disclosure Principle requires that, subject to the conditions in Section 39 of the Act, no personal data may be disclosed without the consent of the data subject for any purpose other than (a) the purpose for which the personal data was to be disclosed at the time of collection of the personal data, or (b) a purpose directly related to that purpose, or (c) to any party other than a third party of the class of third parties specified under the privacy notice.

Notwithstanding the Disclosure Principle, personal data of a data subject may be disclosed by us for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, under the following circumstances. The conditions pursuant to Section 39 of the Act are as follows:-

- (1) The data subject has given his consent to the disclosure.
- (2) The disclosure (a) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations, or (b) was required or authorized by or under any law or by the order of a court.
- (3) We acted in the reasonable belief that we had in law the right to disclose the personal data to the other person. If we have reason to believe that such disclosure is required, we shall discuss this in the first instance with Data Protection Compliance Officer before making the disclosure.
- (4) We acted in the reasonable belief that we would have had the consent of the data subject if the data subject had known of such disclosure and the circumstances of such disclosure. If we have reason to believe that such disclosure is required, we shall discuss this in the first instance with Data Protection Compliance Officer before making the disclosure.
- (5) The disclosure was justified as being in the public interest in the circumstances as determined by the Minister. We will update the Policy from time to time to include new conditions for disclosure.

We shall keep and maintain a list of third parties whom we disclose personal data to.

### ***Principle IV - Security Principle***

When processing personal data, we shall take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. The Security Principle requires us to develop and implement a security policy which involves taking technical and organizational measures to protect personal data which we process.

- (1) Technical measures may include software controls to restrict user access; up-to-date virus checking software; audit trail software; encryption and all of which we have in place and manage through our Information Technology and System Department (ITSM).
- (2) Organizational measures may include restricting access to buildings and computer rooms; ensuring secure disposal of information; and training staff in respect of the care and handling of personal data and all of which we are responsible for complying with and applying to our daily routine.

If we use third parties to process personal data on our behalf, we shall :-

- (1) Ensure that the data processor provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out.
- (2) Take reasonable steps to ensure compliance with those measures by the data processor.

### ***Principle V - Retention Principle***

Personal data processed for any purpose specified in the respective privacy notices must not be kept longer than is necessary for the fulfilment of that purpose. We shall take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed subject to legal requirements to retain the personal data.

### ***Principle VI - Data Integrity Principle***

Personal data must be accurate, complete and up-to-date by having regard to the purpose specified in the respective privacy notices, including any directly related purpose for which the personal data was collected and further processed. Personal data will be inaccurate if they are incorrect or misleading as to any matter of fact (e.g. an incorrect name or address). We shall try to get in touch with the data subject to seek clarification if the accuracy of personal data in our systems is in doubt.

### ***Principle VII - Access Principle***

#### *a. Right to Access and Right of Correction*

We acknowledge that a data subject shall be given access to his personal data held by us and/ or our Data Processors and be able to correct that personal data where it is inaccurate, incomplete and not up-to-date, except where compliance with a request to such access or correction is refused under the Act. We shall endeavour to respond to all access requests within a reasonable time frame and in accordance with our rules and procedures in relation to such requests.

Besides the right to access, all data subjects also have the following rights and we shall address them in accordance with our rules and procedures.

#### *b. Right to prevent processing likely to cause damage or distress*

Data subjects have the right to request that we do not process their personal data in the following circumstances:-

- (i) The processing of the personal data in a particular way or for a particular purpose is causing, or is likely to cause, substantial damage or substantial distress to that data subject or another person.
- (ii) The damage or distress caused is, or would be, unwarranted.

The data subjects will request to exercise his right and ask us to stop processing personal information about himself or another individual.

We will comply with such a request within a reasonable time. Please forward it promptly to our Data Protection Compliance Officer.

#### *c. Right to prevent processing for the purposes of direct marketing*

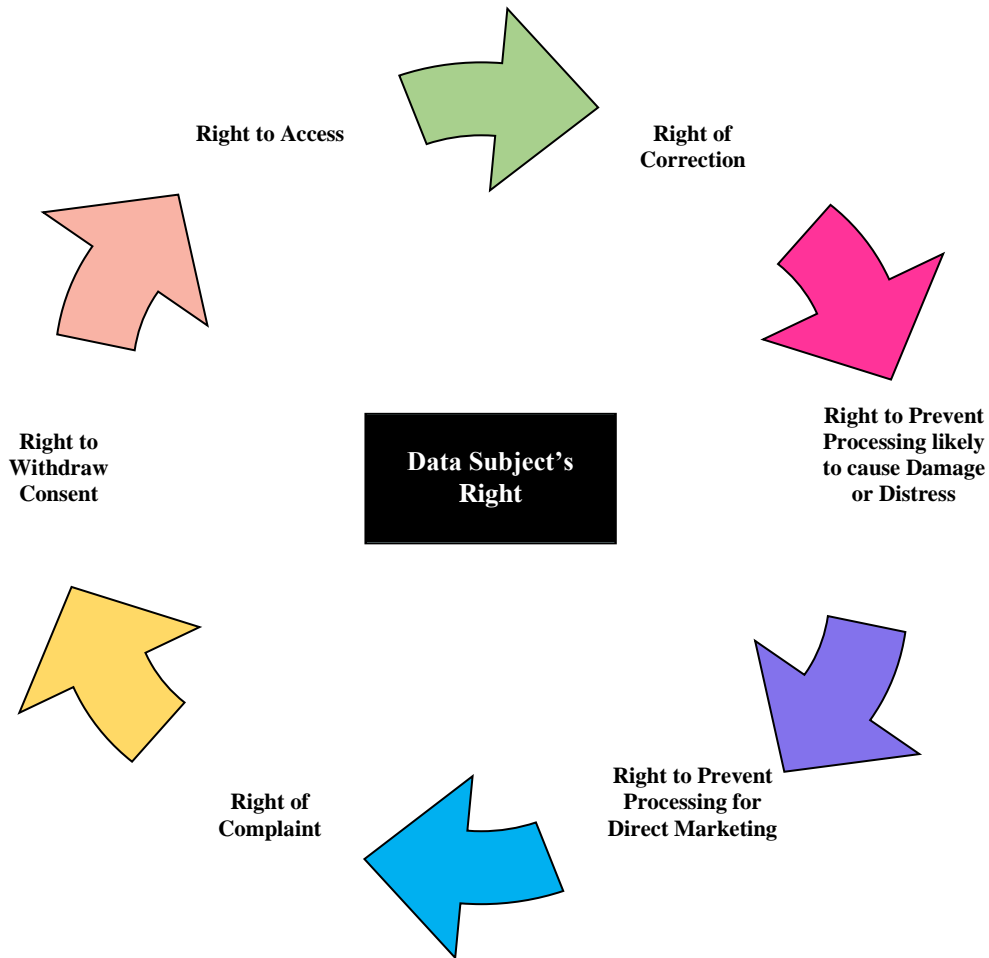
Data subjects have the right to request that we stop processing their personal data for direct marketing purposes. We shall cease sending direct marketing materials to any and all data subjects who have objected to the same.

#### *d. Right of complaint*

Data subjects may channel their complaints in writing, if any, to the Data Protection Compliance Officer about an act, practice or request which may contravene the Act. We shall endeavour to respond and resolve the complaints within a reasonable time frame.

e. Right to withdraw consent

Data subjects may by notice in writing withdraw their consent to the processing of their personal data. Please address the withdrawal request to the Data Protection Compliance Officer.



**C. TRANSFER OF PERSONAL DATA ABROAD**

Transference of any personal data of a data subject to a place outside Malaysia is prohibited unless it is such a place as specified by the Minister<sup>2</sup>. Personal data is only allowed to be transferred to any place outside Malaysia if one of the conditions pursuant to Section 129(1) or Section 129(3) of the Act is met. We shall abide by the following conditions for transfer of personal data abroad:

- (1) The place is a place specified by the Minister by notification published in the Gazette.
- (2) The data subject has given his consent to the transfer.
- (3) The transfer is necessary for the performance of a contract between us and the data subject.
- (4) The transfer is necessary for the conclusion or performance of a contract between us and a third party which (a) is entered into at the request of the data subject or (b) is in the interests of the data subject.
- (5) The transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights.



- (6) We have reasonable grounds for believing that in all circumstances of the case, (a) the transfer is for the avoidance or mitigation of adverse action against the data subject, (b) it is not practicable to obtain the data subject's consent in writing to that transfer, and (c) if it was practicable to obtain such consent, the data subject would have given his consent.
- (7) We have taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the Act.
- (8) The transfer is necessary as being in the public interest in circumstance as determined by the Minister.

#### **E. CONSEQUENCES OF NON-COMPLIANCE**

We view non-compliance with the Act seriously as the consequences for breaching legislation may have severe impact on our business operations. For this reason, it is imperative that we comply with the Policy and the Act.

We have implemented Data Breach Policy to manage data security breach incidents. However, despite all the Policies and Procedures in place, we appreciate the co-operation of all parties concerned to report any breach of personal data to the Data Protection Compliance Officer.

#### **F. INQUIRIES**

Please contact the Data Protection Compliance Officer for any inquiries and complaints in respect of the Policy and/or compliance with the Act in general.

Attention	:	Data Protection Compliance Officer
Address	:	Mewah Group Malaysia Entities Lot 40, Section 4, Fasa 2A Pulau Indah Industrial Park, Jalan Sungai Pinang 5/1, 42920 Pulau Indah, Selangor Darul Ehsan
Telephone No.	:	+603-31693002
Fax No.	:	+603-31011691
E-mail	:	<a href="mailto:PDPA.MALAYSIA@MEWAHGROUP.COM">PDPA.MALAYSIA@MEWAHGROUP.COM</a>

The Policy will be updated from time to time to reflect any changes in the law.

*Note:*

<sup>1</sup> Mewah Group Malaysia Entities (MGMEs) refer to Mewah Group entities incorporated in Malaysia.

<sup>2</sup> The Minister has yet to specify any such place.