Personal Data Protection Act 2010

Highlights of the Personal Data Protection Act 2010 passed by the Malaysian Parliament in May 2010, received Royal Assent on 2 June 2010 and came into force on November 15, 2013 are as follows:

1. **Application.** The Act applies to any person who processes and who has control over or authorises the processing of any personal data in respect of *commercial transactions* and must:
   - be processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
   - be recorded with the intention that it should be processed wholly or partly by such equipment; or
   - be recorded as part of, or with the intention that it should form part of, a relevant filing system; and
   - relate directly or indirectly to a data subject who is identified or identifiable from the information or other information in the possession of a data user.

2. A 'commercial transaction' is defined in section 4 as a transaction of a commercial nature, whether contractual or not, which includes any matter relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.

3. **Non-application.** The Act does not apply to:
   - information processed for the purpose of a credit reporting business under the Credit Reporting Act 2010 as the processing of such information has been specifically excluded from the definition of personal data;
   - Federal Government and State Governments; and
   - Any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.

4. **Personal Data Protection Principles (Section 5).** The Act asserts seven Personal Data Principles which have to be complied with when processing personal data, namely:
   - General Principle;
   - Notice and Choice Principle;
   - Disclosure Principle;
   - Security Principle;
   - Retention Principle;
   - Data Integrity Principle; and
   - Access Principle.
<table>
<thead>
<tr>
<th>Principles</th>
<th>Provisions</th>
</tr>
</thead>
</table>
| General Principle (Section 6) | • A data user is prohibited from processing a data subject’s personal data including sensitive personal data unless with the consent of the data subject.  
• Processing of sensitive personal data, that is 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 similar nature, the commission or alleged commission of any offence or any other personal data as the Minister may determine to be sensitive personal data, must also be in accordance with the provisions of section 40 of the Act.  
• There are however six (6) exceptions where data processing of personal data is necessary and allowed for:  
  − the performance of a contract to which the data subject is a party;  
  − the taking of steps, at the request of the data subject, with a view to entering into a contract;  
  − compliance with any legal obligation to which the data use is the subject, other than an obligation imposed by a contract;  
  − protecting the vital interests of the data subject;  
  − the administration of justice; or  
  − the exercise of any functions conferred on any person by or under any law.  
• Personal data cannot be processed unless:  
  − for lawful purpose directly related to an activity of the data user;  
  − it is necessary for or directly related to that purpose; and  
  − the data is adequate but not excessive in relation to that purpose. |
| Notice and Choice Principle (Section 7) | • The Act requires a data user to inform a data subject by written notice, in both the national and English languages, of the following:  
  − that the personal data of the data subject is being processed and a description of the data;  
  − the purpose for which the personal data is being collected and further processed;  
  − any information available to the data user as to the source of that personal data;  
  − the data subject’s right to request access to and correction of the personal data and contact particulars of the data user in the event of any inquiries or complaints;  
  − the class of third parties to whom the data is or may be disclosed;  
  − the choices and means offered to a data subject to limit the processing of the data; and  
  − whether it is obligatory or voluntary for the data |
subject to supply data, and if obligatory, the consequences of not doing so.

- The notice has to be given by the data user as soon as practicable:
  - when the data user first requests the personal data from the data subject; or
  - when the data user first collects the personal data of the data subject; or
  - before the data user uses the personal data for a purpose other than the purpose for which the data was collected or before the data is disclosed to a third party.

- The data subject must also be provided with a clear and readily accessible means to exercise his choice, where necessary, in the national and English languages.

- Details of the data user to be provided to the data subject in the event of any inquiries or complaints should at least contain the following:
  - designation of the contact person;
  - phone number;
  - fax number (if any);
  - e-mail address (if any); and
  - such other related information.

- Where the data user has complied with the provisions of this Principle in respect of the collection of personal data from the data subject referred to as the “first collection”, the data user is not required to comply with the provisions on any subsequent occasion of collection if the compliance is to repeat in the same circumstances what was done to comply with the principle in respect of the “first collection” and not more than 12 months have elapsed between the first collection and subsequent collection. However a subsequent collection can be considered a first collection if the data user has complied with the provisions of the principle in respect of the subsequent collection.

| Disclosure Principle (Section 8) | • No personal data shall be disclosed without the consent of the data subject for any purpose other than:
  - the purpose for which the personal data was to be disclosed at the time of collection or a purpose directly related to it; or
  - to any party than a third party of the class notified to the data user.
  - The Act under Section 39 provides exceptions to the disclosure of personal data only under the following circumstances:
    - the data subject has given consent to the disclosure;
    - the disclosure is necessary to prevent or detect a crime, or for the purpose of investigations;
    - the disclosure is required or authorised by or under any law or by the order of a court; |
− the data user acted in the reasonable belief that:
  ▪ he had in law the right to disclose the personal data to another person;
  ▪ he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or
  − the disclosure was justified as being in the public interest in circumstances as determined by the Minister.

• The Personal Data Protection Regulations 2013 which came into operations on November 15, 2013 stipulates that a data user shall keep and maintain a list of disclosure to third parties in relation to personal data of the data subject that has been or is being processed by him.

### Security Principle (Section 9)

• The Act requires the data user to take practical steps to protect the personal data when processing from any loss, misuse, modification, unauthorised or accidental access or disclosure, alternation or destruction by having regard:
  − to the nature of the personal data harm that would result if the data is not protected;
  − to the place or location where the data is stored;
  − to any security measures incorporated into any equipment in which the personal data is stored;
  − to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
  − to the measures taken for ensuring the secure transfer of the personal data.

• Where the data processing is carried out by a data processor on behalf of a data user, the data user must ensure that the data processor provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and takes reasonable steps to ensure compliance with those measures.

• The Personal Data Protection Regulations 2013 which came into operations on November 15, 2013 requires the data user to develop and implement a security policy which complies with security standards set out by the Personal Data Protection Commissioner.

### Retention Principle (Section 10)

• The Act stipulates that the personal data processed for any purpose shall not be retained for longer than is necessary for the fulfilment of that purpose. It also imposes a duty on the data users to 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 processed.

• The Personal Data Protection Regulations 2013 which
came into operations on November 15, 2013 requires the personal data of the data subject to be retained in accordance with retention standards set out by the Personal Data Protection Commissioner.

**Data Integrity Principle (Section 11)**

- The data user has to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which it was collected and further processed.
- *The Personal Data Protection Regulations 2013 which came into operations on November 15, 2013 requires the data user to process the personal data of the data subject in accordance with data integrity standards set out by the Personal Data Protection Commissioner.*

**Access Principle (Section 12)**
The Act gives the data subject the right to access his personal data held by a data user and to correct the data where the personal data is inaccurate, incomplete, misleading or not up-to-date. Sections 32 and 36 of the Act respectively, provide grounds where a data user may refuse to comply with the data access and data correction request.

5. **Registration of data users.** The Personal Data Protection (Class of Data Users) Order 2013 which came into operation on November 15, 2013 specifies the following data users to be registered under the Act:

<table>
<thead>
<tr>
<th>Sectors</th>
<th>Class of Data Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications</td>
<td>• A licensee under the Communications and Multimedia Act 1998</td>
</tr>
<tr>
<td></td>
<td>• A licensee under the Postal Services Act 2012</td>
</tr>
<tr>
<td>Banking and financial institution</td>
<td>• A licensed bank and licensed investment bank under the Financial Services Act 2013</td>
</tr>
<tr>
<td></td>
<td>• A licensed Islamic bank and licensed international Islamic bank under the Islamic Financial Services Act 2013</td>
</tr>
<tr>
<td></td>
<td>• A development financial institution under the Development Financial Institution Act 2002</td>
</tr>
<tr>
<td>Insurance</td>
<td>• A licensed insurer under the Financial Services Act 2013</td>
</tr>
<tr>
<td></td>
<td>• A licensed takaful operator under the Islamic Financial Services Act 2013</td>
</tr>
<tr>
<td></td>
<td>• A licensed international takaful operator under the Islamic Financial Services Act 2013</td>
</tr>
<tr>
<td>Health</td>
<td>• A licensee under the Private Healthcare Facilities and Services Act 1998</td>
</tr>
<tr>
<td></td>
<td>• A holder of the certificate of registration of a private medical clinic or a private dental clinic under the Private Healthcare Facilities and Services Act 1998</td>
</tr>
<tr>
<td></td>
<td>• A body corporate registered under the Registration of Pharmacists Act 1951</td>
</tr>
<tr>
<td>Sectors</td>
<td>Class of Data Users</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Tourism and hospitalies | • A licensed person who carries on or operates a tourism training institution, licensed tour operator, travel agent or tourist guide under the Tourism Industry Act 1992  
                          • A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992  |
| Transportation          | • Malaysian Airlines System (MAS)  
                          • MAS Wings  
                          • Berjaya Air  
                          • Air Asia  
                          • Air Asia X  
                          • Firefly  
                          • Malindo Air |
| Education               | • A private higher education institution registered under the Private Higher Educational Institutions Act 1996  
                          • A private school or private educational institution registered under the Education Act 1996 |
| Direct selling          | • A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993  |
| Services                | • A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961 carrying on business as follows:  
                          − Legal  
                          − Audit  
                          − Accountancy  
                          − Engineering  
                          − Architecture  
                          • A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1962, who conducts retail dealing and wholesale dealing as defined under the Control Supplies Act 1961  
                          • A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1962, who carries on business of a private employment agency under the Private Employment Agencies Act 1981. |
| Real estate             | • A licensed housing developer under the Housing Development (Control and Licensing) Act 1966  
                          • A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah  
                          • A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak |
| Utilities               | • Tenaga Nasional Berhad  
                          • Sabah Electricity Sdn Bhd  
                          • Sarawak Electricity Supply Corporation  
                          • SAJ Holdings Sdn Bhd  
                          • Air Kelantan Sdn Bhd  
                          • LAKU Management Sdn Bhd  
                          • PerbadananBekalan Air Pulau Pinang Sdn Bhd  
                          • Syarikat Bekalan Air Selangor Sdn Bhd  
                          • Syarikat Air Terengganu Sdn Bhd  
                          • Syarikat Air Melaka Sdn Bhd  
                          • Syarikat Air Negeri Sembilan Sdn Bhd  
                          • Syarikat Air DarulAman Sdn Bhd  
                          • Pengurusan Air Pahang Berhad  
                          • Lembaga Air Perak  
                          • Lembaga Air Kuching  
                          • Lembaga Air Sibu |
6. Application, certificate, renewal, replacement and revocation of registration.
   
i. Application – A person belonging to the class of data users as specified in the Personal Data Protection (Class of Data Users) Order 2013 must submit an application for registration to the Commissioner in the manner and form determined by the Commissioner, accompanied with the prescribed registration fee and documents specified in the Personal Data Protection (Registration of Data User) Regulations 2013.

   ii. Certificate – Having given due consideration to an application, the Commissioner will issue a certificate of registration to the applicant and where fit may impose certain conditions and restrictions. The certificate has a validity of not less than twelve months from the date of issuance. Any refusal of application for a certificate by the Commissioner will be by way of written notice to the applicant with the reasons for the refusal.

   iii. Renewal – Application for renewal of certificate of registration must be made not later than ninety days before the date of expiry. Renewal application must be in the manner and form as determined by the Commissioner, accompanied with the fee for renewal of certificate of registration as specified in the Schedule in the Personal Data Protection (Registration of Data User) Regulations 2013. When renewing, the Commissioner may vary or impose conditions and restrictions. The Commissioner may refuse to renew a certificate of registration if the data users has failed to comply with the provisions of the Act and conditions and restrictions imposed upon the issuance of the certificate or data user is found unable to continue the processing of personal data in accordance with the Act.

   iv. Replacement – A data user may apply in writing to the Commissioner for a replacement of a certificate of registration if the certificate is lost or damaged. The application must be accompanied with the fee for replacement as specified in the Schedule in the Personal Data Protection (Registration of Data User) Regulations 2013 and a statutory declaration made by the data user to the effect that the certificate issue to him is lost or damaged.

   v. Revocation – The registration of a data user may be revoked if the data user has failed to comply with the provisions of the Act and conditions and restrictions imposed upon the issuance of the certificate, the issuance of the certificate of registration was induced by a false representation of facts by the data user or the data user has ceased to carry on the processing of personal data. A data user will however be given the opportunity to make a representation in writing before the Commissioner revokes the registration.
7. Fees Schedule as per the Personal Data Protection (Registration of Data User) Regulations 2013

<table>
<thead>
<tr>
<th>Establishment of data user</th>
<th>Registration (RM)</th>
<th>Renewal of certificate of registration (RM)</th>
<th>Replacement of certificate of registration (RM)</th>
<th>Certified copy of certificate of registration (each sheet certified) (RM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sole proprietor of a business registered under the Registration of Business Act 1956</td>
<td>100</td>
<td>100</td>
<td>30</td>
<td>10</td>
</tr>
<tr>
<td>Partnership as defined in Section 3 of the Partnership Act 1961</td>
<td>200</td>
<td>200</td>
<td>30</td>
<td>10</td>
</tr>
<tr>
<td>Private company as defined in Section 4 of the Companies Act 1965</td>
<td>300</td>
<td>300</td>
<td>30</td>
<td>10</td>
</tr>
<tr>
<td>Public company as defined in Section 4 of the Companies Act 1965</td>
<td>400</td>
<td>400</td>
<td>30</td>
<td>10</td>
</tr>
</tbody>
</table>

8. Rights of a data subject - The Act confers the following rights on a data subject vis-à-vis a data user in relation to his personal data and the processing thereof:

- **The right of access to personal data (Section 30)**
  - An individual has the right, upon a written request and payment of a prescribed fee, to be informed by a data user as to whether personal data of which that individual is the data subject is being processed by or on behalf of the data user.
  - A data user must comply with the data access request not later than 21 days from the date of receipt of the data access request and if unable to comply within the specified period must before the expiration of the period inform the requestor in writing of his inability to comply with the request and the reasons why he is unable to do so and comply with the request to the extent that he is able to do so.
  - Notwithstanding the above, the data user shall comply in whole with the data access request within a further 14 days after the expiration of the initial 21-day period.
  - The data user may refuse to comply with the data access request on the following grounds:
    i. where the data user is not supplied with sufficient information as to the identity of the requestor or of the relevant person making the request;
    ii. where the data user is not supplied with sufficient information to enable him to locate the personal data;
    iii. where the burden or expense of providing access is not proportionate to the risk of the data subject’s privacy;
    iv. where the data user cannot comply with the request without disclosing the personal data of another individual who is identifiable from that information unless the other individual has consented to the disclosure of the information or it is reasonable in all circumstances to comply with the data access request without the consent of the other individual;
v. the processing of personal data is controlled by another data user in a manner which prohibits the relevant data user from complying in whole or part with the request;
vi. where providing access would constitute a violation of an order of a court;
vii. where providing access would disclose confidential commercial information; or
viii. where the access is regulated by another law.

• The right to correct personal data (Section 34)
  − A requestor or a data subject is entitled to request for a correction of his personal data if he knows or considers his personal data held or supplied by the data user to be inaccurate, incomplete, misleading or not up-to-date.
  − If the data user is satisfied that the data should be corrected, he shall do all of the following within 21 days from the day of receipt of the request:
    i. correct the personal data;
    ii. supply a corrected copy to the data subject or the requestor; and
    iii. take steps to supply a third party with a corrected copy of the personal data with a notice stating the reasons for such correction if:
        a) the personal data has been disclosed to that third party within 12 months preceding the day on which the correction is made; and
        b) the data user believes that the third party has not ceased to use the data for the purpose for which it was disclosed including for any directly related purpose.
  − If the data user is unable to comply with the request within the specified time, he must notify the requestor in writing of his inability to do so (and the reasons therefor) before the expiry of the 21-day period. The data user must, however, comply with the request to the extent that he is able to do so within that time period
  − The data user must then comply fully with the data correction request within a period of 14 days after the expiry of the initial 21 day period.
  − The data user may refuse to comply with the data correction request on the following grounds
    i. where the data user is not supplied with sufficient information as to the identity of the requestor or of the relevant person making the request;
    ii. where the data user is not supplied with such information as to enable him to ascertain the manner in which the personal data is inaccurate, incomplete, misleading or outdated;
    iii. where the data user is not satisfied that the personal data which is required to be corrected is inaccurate, incomplete, misleading or not up-to-date;
    iv. where the data user is not satisfied that the correction requested for is accurate, complete, not misleading or up-to-date; or
    v. where the processing of personal data is controlled by another data user in a manner which prohibits the relevant data user from complying in whole or part with the data correction request.
  − A data user who, refuses to comply with a data correction request must within 21 days from receipt of the request, inform the requestor of the refusal and the reasons therefor. Where a request is refused on the grounds where processing of personal data is controlled by another data user in a manner which prohibits the relevant data user from complying in whole or part with the request, the data user must provide the requestor with the name and address of the other data user concerned.
  − If the data correction request relates to an expression of opinion and the data user is not satisfied that the opinion expressed is inaccurate, incomplete, misleading or not up-to-date, he must:
i. make a note which is to be annexed to the personal data or elsewhere of the matters in respect of which the requestor deems the opinion expressed to be inaccurate, incomplete, misleading or not up-to-date; and

ii. ensure that the relevant data cannot be used by any person without his attention being drawn to the note

iii. Attach a copy of the note to the notice of refusal which he issues to the requestor.

- **Right to withdraw consent to process personal data (Section 38)** - A data subject may, by written notice to a data user, withdraw his consent to the processing of his personal data. The data user shall cease processing the personal data of such data subject upon receipt of the notice.

- **Right to prevent processing likely to cause damage or distress (Section 42)**
  
  - A data subject may, by way of a data subject notice in writing require a data user to cease or not begin the processing of personal data for a specified purpose or in a specified manner which, based on the reasons stated by the data subject, may or is likely to cause substantial damage or substantial distress to him or to another person which is or would be unwarranted. This however shall not apply where:
    
    i. the data subject had given his consent;
    
    ii. the processing is necessary for:
        
        ▪ the performance of a contract to which the data subject is a party;
        
        ▪ the taking of steps at the request of the data subject with a view to entering a contract;
        
        ▪ compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by contract; or
        
        ▪ the protection of the vital interest of the data subject.
    
  
  - A data user shall within 21 days from the date of receipt of the data subject notice, give the data subject a written notice stating:
    
    i. that he has complied or intends to comply with the notice; or
    
    ii. the reasons for regarding the data subject notice as unjustified or to any extend unjustified and the extent, if any, to which he has complied or intends to comply with the notice.

  
  - A data user shall within 21 days from the date of receipt of the data subject notice, give the data subject a written notice stating:
    
    A data subject who is not satisfied with the data user’s response may submit an application to the Commissioner to require the data user to comply with his request. The Commissioner may direct the data user to comply with the request to the extent that the Commissioner deems justified.

- **Right to prevent processing for direct marketing (Section 43)**
  
  - A data subject may, by way of written notice, require a data user at the end of such period as is reasonable, to cease or not to begin processing his personal data for the purposes of direct marketing:
    
    If the data user refuses to comply with the notice, the data subject may apply to the Commissioner to require the data user to comply with the notice. The Commissioner may require the data user to comply with the notice to the extent that the Commissioner deems justified.
9. **Processing of sensitive personal data (Section 40)**

- A data user shall not process any sensitive personal data of a data subject except in the following conditions:
  - the data subject has given his explicit consent to the processing of the personal data;
  - the processing is necessary:
    i. for the purpose of exercising or performing an right or obligation which is conferred or imposed by law on the data user in connection with employment;
    ii. in order to protect vital interests of the data subject or another person where consent cannot be given by or on behalf of the data subject or the data user cannot reasonably be expected to obtain the consent of the data subject;
    iii. in order to protect the vital interests of the another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
    iv. for medical purposes and is undertaken by healthcare professionals or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;
    v. for the purpose of or in connection with any legal proceedings;
    vi. for the purpose of obtaining legal advice;
    vii. for the purpose of establishing, exercising or defending legal rights;
    viii. for the administration of justice;
    ix. for the exercise of any functions conferred on any person by or under any written law;
    or
    x. for any other purposes as the Minister thinks fit; or
  - the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject

- The Minister may by order published in a gazette exclude the application of items (i), (viii) or (ix) which would be specified in the order.

10. **Penalties** are applicable for the following offences by a data user:

<table>
<thead>
<tr>
<th>Offences</th>
<th>Sections</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data Protection Principles</td>
<td>6-12</td>
<td>• Fine ≤ RM 300,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 2 years; or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Certificate of registration</td>
<td>16</td>
<td>• Fine ≤ RM 500,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 3 years; or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Revocation of registration</td>
<td>18</td>
<td>• Fine ≤ RM 500,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 3 years; or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Surrender of certificate of registration</td>
<td>19</td>
<td>• Fine ≤ RM 200,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 2 years; or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Non-compliance with code of practice</td>
<td>29</td>
<td>• Fine ≤ RM 100,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 1 years; or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Notification of refusal to comply with data correction request</td>
<td>37(2)</td>
<td>• Fine ≤ RM 100,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 1 years; or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Offences</td>
<td>Sections</td>
<td>Penalty</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Withdrawal of consent to process personal data</td>
<td>38(2)</td>
<td>• Fine ≤ RM 100,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 1 years;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Processing on sensitive personal data</td>
<td>40</td>
<td>• Fine ≤ RM 200,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 2 years;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Right to prevent processing likely to cause damage or distress</td>
<td>42(5)</td>
<td>• Fine ≤ RM 200,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 2 years;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Right to prevent processing for purposes of direct marketing</td>
<td>43(3)</td>
<td>• Fine ≤ RM 200,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 2 years;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Enforcement notice</td>
<td>108</td>
<td>• Fine ≤ RM 200,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 2 years;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Search and seizure with warrant</td>
<td>13(6)</td>
<td>• Fine ≤ RM 50,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 6 mths;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Obstruction to search</td>
<td>120</td>
<td>• Imprisonment ≤ 2 years;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fine ≤ RM 10,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
<tr>
<td>Unlawful collection, etc of personal data</td>
<td>130</td>
<td>• Fine ≤ RM 500,000;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Imprisonment ≤ 3 years;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Both</td>
</tr>
</tbody>
</table>

The Commissioner may, with the consent in writing of the Public Prosecutor, compound any offence committed by any person under this Act and prescribed to be a compoundable offence by making a written offer to the persons suspected to have committed the offence to compound the offence upon payment to the Commissioner of an amount not exceeding 50% of the amount of maximum fine for that offence.

11. Other Key Provisions

- **Commissioner** – The Act Provides for the appointment and sets out the functions and powers of a Personal Data Protection Commissioner. His functions include advising the Minister on the national policy for data protection and implementing and enforcing data protection laws. Encik Abu Hassan bin Ismail was appointed as the Personal Data Protection Commissioner by the Minister with effect from November 15, 2013.

- **Data User Forum and Code of Practice** - The Commissioner may, with the agreement of a body, designate that body to be a data user forum for a specific class of data users. A data user forum may upon its own initiative or at the request of the Commissioner, prepare a code of practice. The Commissioner may also opt to issue such a code if one is not prepared by the relevant forum. Data users are under obligation to comply with the relevant code of practice. The failure to do so constitutes a statutory offence.

- **Advisory Committee** - The Act establishes a Personal Data Protection Advisory Committee. The functions of the Committee are to advise the Commissioner on all matters relating to personal data protection, the administration of the Act and any other matter referred to them by the Commissioner. The Commissioner is not bound by the advice of the Committee.
• **Appeal Tribunal** - The Act establishes an Appeal Tribunal. The powers of the Tribunal include hearing of appeals lodged with them by any person who is aggrieved by the decision of the Commissioner. The procedures for an appeal are set out in the Act. The decision of the Tribunal is final and binding on the parties to an appeal and may, with leave of the Sessions Court, be enforced in the same manner as a judgment or order, and be entered as a judgment.

Prepared by: Federation of Malaysian Manufacturers

January 13, 2014