KKMM
KEMENTERIAN KOMUNIKASI
DAN MULTIMEDIA MALAYSIA

PERSONAL
DATA PROTECTION
COMMISSIONER MALAYSIA
Ministry of Communication and
Multimedia Malaysia

WHAT YOU NEED TO KNOW?

PERSONAL DATA PROTECTION ACT 2010 (ACT 709)

www.pdp.gov.my

BACKGROUND

Personal Data Protection Act 2010 (Act 709), an Act to regulate the processing of personal data in commercial transaction and to provide for matters connected therewith and incidental thereto. Personal Data Protection Act 2010 ('PDPA'), was passed by the Malaysian Parliament on 2 June 2010 and came into force on 15 November 2013.

DEFINITION OF PERSONAL DATA

Personal data means any information in respect of commercial transactions, which:

is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose

or

is recorded with the intention that it should wholly or partly be processed by means of such equipment, or

or

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.

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister of Communications and Multimedia Malaysia (*'Minister'*) may determine by order published in the Gazette. Other than the categories of sensitive personal data listed above, the Minister has not *'Gazetted'* any other types of personal data to be sensitive personal data as of 29 December 2014.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to the PDPA, a Personal Data Protection Commissioner (*'Commissioner'*) has been appointed to implement the PDPA's provisions. The Commissioner will be advised by a Personal Data Protection Advisory Committee who will be appointed by the Minister, and shall consist of one Chairman, three members from the Public sector, and at least seven but no more than eleven other members. The appointment of the Personal Data Protection Advisory Committee shall not exceed a term of three years, however members can be appointed for two terms in succession.

DECISIONS OF THE COMMISSIONER CAN BE APPEALED AGAINST THROUGH THE PERSONAL DATA PROTECTION APPEAL TRIBUNAL. THESE ARE DECISIONS SUCH AS:

- Decisions relating to the registration of data users under Part II Division 2 of the PDPA
- The refusal of the Commissioner to register a code of practice under Section 23(5) of the PDPA
- The service of an enforcement notice under Section 108 of the PDPA
- The refusal of the Commissioner to vary or cancel an enforcement notice under Section 109, or
- The refusal of the Commissioner to conduct or continue an investigation which is based on a complaint under Part VIII of the PDPA.

If a data user is not satisfied with a decision of the Personal Data Protection Advisory Committee, the data user may proceed to file a judicial review of the decision in the Malaysian High Courts.

REGISTRATION

Registration of data users are pursuant to Section 14 of the PDPA. Currently, the PDPA requires certain classes of data user to be registered under the Act. However, the list is not exhaustive and therefore additional classes of data user may be added from time to time. The class of data users that requires to register are as follows:

COMMUNICATIONS

1. A licensee under the Communications and Multimedia Act 1998
2. A licensee under the Postal Services Act 2012

BANKING AND FINANCIAL INSTITUTION

1. A licensed bank and licensed investment bank under the Financial Services Act 2013
2. A licensed islamic bank and licensed international islamic bank under the Islamic Financial Services Act 2013
3. A development financial institution under the Development Financial Institution Act 2002

INSURANCE

1. A licensed insurer under the Financial Services Act 2013
2. A licensed takaful operator under the Islamic Financial Services Act 2013
3. A licensed international takaful operator under the Islamic Financial Services Act 2013

HEALTH

1. A licensee under the Private Healthcare Facilities and Services Act 1998
2. 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
3. A body corporate registered under the Registration of Pharmacists Act 1951

TOURISM AND HOSPITALITIES

1. A licensed person who carries on or operates a tourism training institution, licensed tour operator, licensed travel agent or licensed tourist guide under the Tourism Industry Act 1992
2. A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992.

TRANSPORTATION

1. Malaysian Airlines System (MAS)
2. Air Asia
3. MAS Wings
4. Air Asia X
5. Firefly
6. Berjaya Air
7. Malindo Air

REAL ESTATE

1. A licensed housing developer under the Housing Development (Control and Licensing) Act 1966
2. A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah
3. A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak

UTILITIES

1. Tenaga Nasional Berhad
2. Sabah Electricity Sdn. Bhd
3. Sarawak Electricity Supply Corporation
4. SAJ Holding Sdn. Bhd
5. Air Kelantan Sdn. Bhd
6. LAKU Management Sdn. Bhd
7. Perbadanan Bekalan Air Pulau Pinang Sdn. Bhd
8. Syarikat Bekalan Air Selangor Sdn. Bhd
9. Syarikat Air Terengganu Sdn. Bhd
10. Syarikat Air Melaka Sdn. Bhd
11. Syarikat Air Negeri Sembilan Sdn. Bhd
12. Syarikat Air Darul Aman Sdn. Bhd
13. Pengurusan Air Pahang Berhad
14. Lembaga Air Perak
15. Lembaga Air Kuching
16. Lembaga Air Sibu

Non-compliance of Section 14 commits an offence and shall, on conviction, be liable to a fine not exceeding RM500, 000 or to imprisonment for a term not exceeding 3 years or both.

The certificate of registration is valid for a period of one year (currently, the Commissioner grants the validity period of two years) and a data user who fails to renew a certificate of registration and continues to process personal data after the expiry date commits an offence and shall, on conviction, be liable to a fine not exceeding RM250, 000 or to imprisonment for a term not exceeding 2 years or both.

Data users are also required to display their certificate of registration at a conspicuous place at their principle place of business, and a copy of the certificate for each branch, where applicable.

EDUCATION

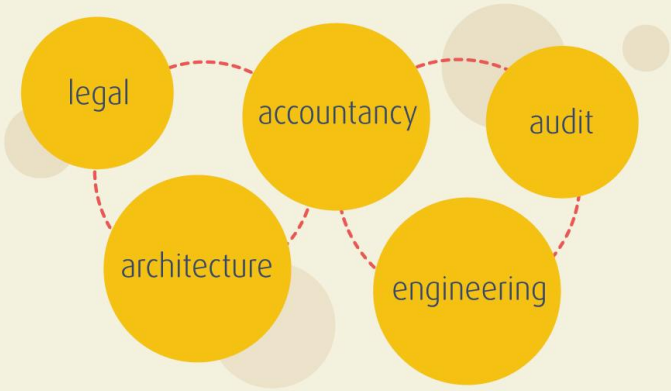
1. A private higher educational institution registered under the Private Higher Educational Institutions Act1996
2. A private school or private educational institution registered under the Education Act 1996

DIRECT SELLING

A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993

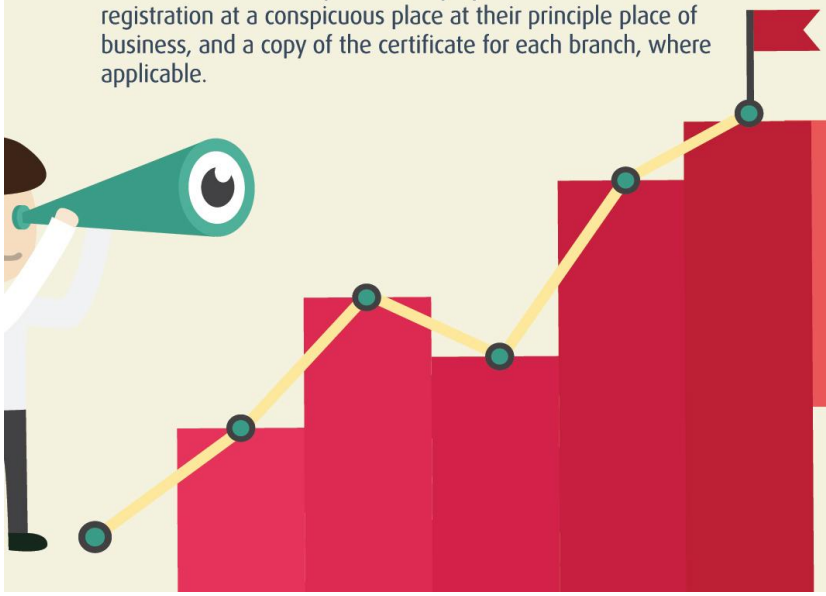
SERVICES

1. 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:



2. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who conducts retail dealing and wholesale dealing as defined under the Control Supplies Act 1961

3. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who carries on the business of a private employment agency under the Private Employment Agencies Act 1981



**Companies who do not belong to a class of Data Users but processes personal data in commercial transaction shall also comply with the provisions stipulated under the PDPA except registration.*

PERSONAL DATA PROTECTION PRINCIPLES

The PDPA asserts seven Personal Data Protection Principles which have to be complied with when processing personal data, namely:

1. **General Principle**
The General Principle prohibits a data user from processing a data subject's personal data without his/her consent.

2. **Notice and Choice Principle**
The PDPA requires a data user to inform a data subject by written notice, in both the national and English languages; of various matters relating to the information of that data subject which is being processed by or on behalf of that data user and provide means of choice to the data subject.

3. **Disclosure Principle**
This Principle prohibits the disclosure, without the data subject's consent, of personal data.

4. **Security Principle**
The PDPA imposes obligations on the data user to take steps to protect the personal data during its processing from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

5. **Retention Principle**
Under this Principle, personal data is not to be retained longer than is necessary for the fulfilment of the purpose for which it was processed. Once the purpose has been fulfilled, it is the duty of a data user to take reasonable steps to ensure that the data is destroyed or permanently deleted.

6. **Data Integrity Principle**
It is the responsibility of a data user to t a k e reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept-up-to-date, having regard to the purpose (and any directly related purpose) for which it was collected and processed.

7. **Access Principle**
The PDPA gives the data subject the right to access his/her own data and to correct the personal data which is inaccurate, incomplete, misleading or outdated. Nevertheless, the PDPA provides grounds on which the data user may refuse to comply with a data access request or data correction request by the data subject.

DATA USER FORUM

The Commissioner may designate a body as a data user forum in respect of a class of data users. The Data user forum may prepare codes of practice on its own initiatives or upon request by the Commissioner to govern the compliance of the PDPA. Once the code of practice is registered, all data users must comply with the provisions of the code, and non-compliance is an offence under the PDPA.

Therefore, companies may want to consider participating in such data user forum to take part in shaping the codes of practice, as this provides them with an opportunity to influence the codes of practice which companies will ultimately have to comply with.

CODE OF PRACTICE

The Code of Practice is issued pursuant to Section 23 of the PDPA. This Code aims to further inculcate the spirit and practice of ethical business within the industry while providing a self-regulating mechanism for collection, maintenance, retention and disposal of personal data. The views of data users, data subjects and the relevant regulatory authority are also taken into consideration in preparing the respective Code of Practice.

Objectives

The Code of Practice is intended to:-

i. Set minimum standards of conduct in respect of personal data that are expected of Data Users;

ii. Stipulate measures to be deployed by Data Users in order to ensure that the processing of personal data does not infringe a Data Subject's rights under the Act;

iii. Stipulate matters for the consideration of Data Users in order to ensure that the risk to the personal data of Data Subject's is minimized; and

iv. Establish the administrative framework to oversee and enforce compliance of Data Users with this Code.

Scope

The Code of Practise shall apply to all businesses processing of personal data in a commercial transaction in Malaysia.

This Code shall apply to all relations between Data Users and individuals whose personally-identifiable information is processed by the Data User as part of or in contemplation of one or more commercial transactions. This includes, but is not limited to, relationships between Data Users and the following individuals:-

(i) individuals who are (or were) customers of Data Users;

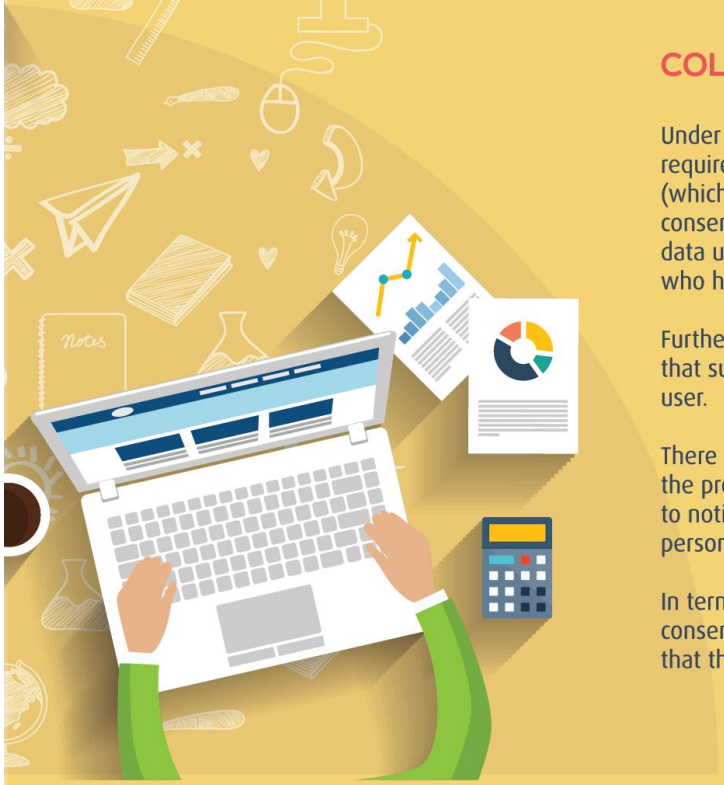
(ii) individuals that represent customers of Data Users (e.g. parents of minors, and authorised representatives);

(iii) individuals that have been identified as potential customers of Data Users;

(iv) individuals that have applied to be customers of a Data User, whether successfully or otherwise;

(v) individuals who are not customers of a Data User but utilise (or have utilised) the facilities or service provided by the Data User; and

(vi) individuals that have entered into ancillary arrangements with a Data User (e.g. guarantors or third party security providers) on account or for the benefit of another individual or entity.



COLLECTION & PROCESSING

Under the PDPA, subject to certain exceptions, data users are generally required to obtain the consent of data subjects for the processing (which includes collection and disclosure) of their personal data. Where consent is required from a data subject under the age of eighteen, the data user shall obtain consent from the parent, guardian, or person who has parental responsibility on the data subject.

Further, the consent obtained from a data subject must be in a form that such consent can be recorded and maintained properly by the data user.

There are also other obligations imposed on the data user in relation to the processing of personal data, including, for example, requirements to notify the data subjects regarding the purpose for which their personal data are collected.

In terms of disclosure to third parties, in addition to obtaining the consent of the data subject for such disclosure, data users must ensure that they keep and maintain a list of the disclosures to third parties.

TRANSFER

Under the PDPA, a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister.

However, there are exceptions to this restriction, such as where:

- Consent has been obtained from the data subject for the transfer;
- The transfer is necessary for the purpose of legal proceedings or to obtain legal advice; and
- The transfer is necessary for the performance of a contract between the data subject and the data user;
- The transfer is necessary to protect the data subject's vital interest and for the public's interest.

ENFORCEMENT

Under the PDPA, the Commissioner is empowered to implement and enforce the personal data protection laws and to monitor and supervise compliance with the provisions of the PDPA. Under the Personal Data Protection Regulations 2013, the Commissioner has the power to inspect the personal data system and the data user is required, at all reasonable times, to open the personal data protection system for inspection by the Commissioner or any inspection officers. The Commissioner or the inspection officers may require the production of the following during inspection:

1) **General Principle**
   The record of the consent from a data subject maintained in respect of the processing of personal data by the data user;

2) **Notice and Choice Principle**
   The record of a written notice issued by the data user to the data subject;

3) **Disclosure Principle**
   The list of disclosure to third parties in respect of personal data that has been or is being processed by him;

4) **Security Principle**
   The security policy developed and implemented by the data user;

5) **Retention Principle**
   The record of compliance in accordance with the retention standard;

6) **Data Integrity Principle**
   The record of compliance in accordance with the data integrity standard; and

7) **Such other** related information which the Commissioner or any inspection officer deems necessary.

Violation of the PDPA and certain provisions of the Personal Data Protection Regulations 2013 attracts criminal liability.

The prescribed penalties include the imposition of fines or a term of imprisonment, or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defence.

However, there is no express right under the PDPA allowing aggrieved data subjects to pursue a civil claim against data users for breaches of the PDPA.

ELECTRONIC MARKETING

The PDPA applies to electronic marketing activities that involve the processing of personal data for the purposes of commercial transactions. There are no specific provisions in the PDPA that deal with electronic marketing. However, the PDPA provides that a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing. 'Direct marketing' means the communication by whatever means of any advertising or marketing material which is directed to particular individual.

ONLINE PRIVACY

There are no provisions in the PDPA that specifically address the issue of online privacy (including cookies and location data). However, any electronic processing of personal data in Malaysia will be subject to the PDPA and the Commissioner may issue further guidance on this issue in the future.

SECURITY

Under the PDPA, data users have an obligation to take 'practical' steps to protect personal data and in doing so shall develop and implement a security policy. The Commissioner may also from time to time set out security standards which the data user must comply with, and the data user is required to ensure that its data processors also comply with these security standards.

Personal Data Protection Standard 2015 (PDP Standard)

Traditionally, data breach can occur by means such as scrap papers and phone calls. However, in this day and age, hacking of computers and servers can also contribute to data breach incidents.

Data breaches can be avoided if appropriate measures are taken in guarding personal data. Therefore, in order to guide data users, the Commissioner of Personal Data Protection (Commissioner) has issued the Personal Data Protection Standard 2015 (PDP Standard).

The PDP Standard is a minimum standard which comprises of three personal data protection principles namely security, retention and data integrity. Out of the seven principles of personal data protection, these three principles are highly regarded as the most vulnerable to breaches.

In terms of security, data users are required to take practical steps when processing personal data.

As such, data user must set the limit of access to personal data system. This is to safeguard the level of access to personal data.

As for retention, personal data shall not be kept longer than necessary unless there are other provisions of the law which requires it to be kept longer.

Finally, for data integrity, the data user shall ensure that personal data is accurate, complete, current and not misleading. The updating of personal data must be performed immediately upon request by the data subject. This is to ensure that the data subject's personal data is accurate and correct at time of his request.

EXEMPTIONS

The PDPA provides certain exemptions from the application of the PDPA

SECTION	PROCESSING ACTIVITY	EXEMPTION
45(1)	**Personal, family or household affairs** Personal data processed by an individual only for the purposes of an individual's personal, family or household affairs, including recreational purposes.	Total exemption
45(2)(a)	**Crime and taxation** Personal Data processed for : (i) The prevention or detection of crime (ii) For the purpose of investigation (ii) The apprehension or prosecution of offenders; or (iii) The assessment or collection of any tax or duty or any other imposition of a similar nature.	General Principle; Notice and Choice Principle; Disclosure Principle; and Access Principle
45(2)(b)	**Physical and mental health** Personal data processed in relation to information of the physical or mental health of a data subject.	Access Principle
45(2)(c)	**Research and statistics** Personal data processed for preparing statistics or carrying out research, provided such personal data is not processed for any other purpose and that the resulting statistics or the result of the research are not made available in a form which identifies the data subject.	General Principle; Notice and Choice Principle; Disclosure Principle; and Access Principle
45(2)(d)	**Order or judgement of a court** Personal data that is necessary for the purpose of or in connection with any order or judgment of a court.	General Principle; Notice and Choice Principle; Disclosure Principle; and Access Principle
45(2)(e)	**Discharge of regulatory functions** Personal data processed for the purpose of discharging regulatory functions.	General Principle; Notice and Choice Principle; Disclosure Principle; and Access Principle
45(2)(f)	**Journalism, literature and art** Personal data processed only for journalistic, literary or artistic purposes provided the following three conditions are satisfied: (i) The processing is undertaken with a view to the publication by any person of the journalistic, literary, or artistic material; (ii) The data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; (iii) The data user reasonably believes that in all the circumstances, compliance with the provisions in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.	General Principle; Notice and Choice Principle; Disclosure Principle; Retention Principle; Data Integrity Principle; and Access Principle

OFFENCES

The PDPA creates a number of criminal offences for the failure to comply with the provisions under the PDPA.

SECTION/RULE	OFEENCES	PENALTY
Section 5(2) Personal Data Protection Principle	Failure to comply with any of the PDPA principles	Fine not exceeding RM300,000; or imprisonment for a term not exceeding 2 years; or both
Section 16(4) Certificate of registration	Processing personal data by data user specified in the order made under subsection 14(1) without a certificate of registration issued by the Commissioner	Fine not exceeding RM500,000; or imprisonment for a term not exceeding 3 years; or both.
Section 18(4) Revocation of registration	Continue to process personal data after the registration is revoked	Fine not exceeding RM500,000; or imprisonment for a term not exceeding 3 years; or both.
Section 19(2) Surrender of certificate of registration	Failure to surrender the certificate of registration to the Commissioner after it is revoked	Fine not exceeding RM200,000; or imprisonment for a term not exceeding 2 years; or both.
Section 29 Non-compliance with code of practice	Failure to comply with any provision of the code of practice that is applicable to the data user	Fine not exceeding RM100,000; or imprisonment for a term not exceeding 1 year; or both.
Section 37(4) Notification of refusal to comply with data correction request	A data user who contravenes section 37(2) of the Act.	Fine not exceeding RM100,000-00; or imprisonment for a term not exceeding 1 year; or both.
Section 38(4) Withdrawal of consent to process personal data	Continue to process personal data after withdrawal of consent by the data subject	Fine not exceeding RM100,000; or imprisonment for a term not exceeding 1 year; or both.
Section 40(3) Processing of sensitive personal data	Processing sensitive personal data without complying with the conditions stated under Section 40(1)	Fine not exceeding RM200,000-00; imprisonment for a term not exceeding 2 years; or both.

SECTION/RULE	OFEENCES	PENALTY
Section 42(6) Right to prevent processing likely to cause damage or distress	Failure to comply with the Commissioner's requirement to cease processing personal data that is likely to cause damage or distress	Fine not exceeding RM200,000; imprisonment for a term not exceeding 2 years; or both.
Section 43(4) Right to prevent processing for purpose of direct marketing	Failure to comply with the Commissioner's requirement to cease processing personal data for the purposes of direct marketing	Fine not exceeding RM200,000; imprisonment for a term not exceeding 2 years; or both.
Section 108(8) Enforcement notice	Failure to comply with an enforcement notice.	Fine not exceeding RM200,000; imprisonment for a term not exceeding 2 years; or both.
Section 129(5) Transfer of personal data to place outside Malaysia	Transfer any personal data to a place outside Malaysia which has not been specified by the Minister and published in the Gazette	Fine not exceeding RM300,000; imprisonment for a term not exceeding 2 years; or both.
Section 130(3) Unlawful collecting etc., personal data	Unlawfully collect or disclose of personal data or procure the disclosure of personal data that is held by the data user without the consent of the data user	Fine not exceeding RM500,000; imprisonment for a term not exceeding 3 years; or both.
130(4) and (5)	Sale or offer to sell personal data	Fine not exceeding RM500,000; imprisonment for a term not exceeding 3 years; or both.
Section 131(1) & (2) Abetment and attempt punishable as an offence	Abet the commission of, or attempts to commit, or does any act preparatory to in furtherance of the commission of any offence under the PDPA	Be liable to the punishment provided for that offence provided that any term of imprisonment imposed shall not exceed one-half of the maximum term provided for the offence.

RIGHTS OF THE DATA SUBJECTS

The PDPA confers rights on a data subject in relation to his personal data. Such rights include:

SECTION	RIGHT	EXPLANATORY STATEMENT
30	Right of access to personal data	A data subject is entitled to be informed by a data user whether his personal data is being processed by or on behalf of the data user. A requester (the data subject or the relevant person on behalf of the data subject) may, upon payment of a prescribed fee, make a data access request in writing to the data user for information of the data subject's personal data that is being processed and to have communicated to him a copy of the personal data in intelligible form.
34	Right to correct personal data	Where a copy of the personal data has been supplied by the data user in compliance with the data access request and the requestor considers or the data subject knows that the personal data inaccurate, incomplete, misleading or not up-to-date, the requester or the data subject may make a data correction request in writing to the data user that the data user make the necessary correction to the personal data.
38	Right to withdraw consent	A data subject may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject. The data user shall, upon receiving the notice, cease the processing of the personal data.
42	Right to prevent processing likely to cause damage or distress	A data subject may, anytime by notice in writing to a data user, require the data user to cease or not begin the processing of the processing for a specified purpose or in a specified manner, of any personal data based on the reasons that the processing of that personal data is causing or likely to cause substantial damage or substantial distress to him or to another; and the damage or distress is or would be unwarranted.
43	Right to prevent processing for purposes of direct marketing	A data subject may, anytime by notice in writing to a data user, require the data user to cease or not begin processing his personal data for purposed of direct marketing. * *Direct marketing is defined as the communication by whatever means of any advertising or marketing material which is directed to a particular individuals.*

HOW TO LODGE A COMPLAINT?

A complaint about data breach:
The Data Protection Commissioner will help you in ensuring that your legal rights are fully upheld, and that organisations meet their obligations under the PDPA. If you think that a person or organisation is not meeting their data protection obligations, and if you are not satisfied with their response to your concerns, then you may complain to the Commissioner.

Making a complaint is simple and free. All you need to do is write to the Data Protection Commissioner, giving details about the matter. You should clearly identify the organisation or individual you are complaining about. You should also outline the steps you have taken to have your concerns dealt with by the organisation, and what sort of response you received from them. Please also provide copies of any letters between you and the organisation, as well as supporting evidence/material.

A complaint about unsolicited direct marketing:
It is not an offence for a marketer to call you at the first time for marketing purposes unless you have clearly not consented to the receipt of such calls.

When making a complaint, you should provide as much information as possible, including your own personal details; time and date of the marketing message, e-mail or letter being received; a copy of the message, or a summary of contents; information about any previous dealing with the sender of that marketing message as well as a statement that you are making a formal complaint.

A complaint about data breach or unsolicited direct marketing can be made in writing to:-

Commissioner of Personal Data Protection
6th Floor, KKMM Complex, Lot 4G9, Persiaran Perdana,
Precint 4, Federal Government Administrative Centre
62100 Putrajaya Federal Territory
T: 03.8000.8000

Complaint/inquiry: aduan@pdp.gov.my
www.facebook.com/JabatanPerlindunganDataPeribadi
* *complaints unrelated with commercial transaction are not covered under this Act*