



PESURUHJAYA
PERLINDUNGAN DATA
PERIBADI MALAYSIA

Kementerian Komunikasi
dan Multimedia Malaysia

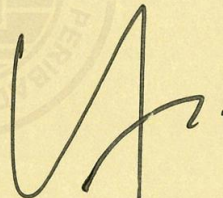
GENERAL CODE OF PRACTICE OF PERSONAL DATA PROTECTION

PESURUHJAYA PERLINDUNGAN DATA PERIBADI

| |
|----------|
| Ref.No. |
| CoP_Umum |

IN exercise of the powers conferred by Section 24(1) of the Personal Data Protection Act 2010 [Act 709], I hereby register the General Code of Practice for the said Class of Data Users and it is applicable to all Data Users with immediate effect.

Dated : 15 December 2022



(MAZMALEK BIN MOHAMAD)
Personal Data Protection Commissioner, Malaysia



FOREWORD

This General Code of Practice of Personal Data Protection aims to enforce compliance to Section 23 of the Personal Data Protection Act [Act 709], regulations and standard and establish a guideline to the Class of Data Users who have not prepared a Code of Practice and there is no data user forum to develop the relevant Code of Practice for the Class of Data Users. Should you require further information, kindly consult —

The Personal Data Protection Commissioner at —

6th Floor, KKMM Complex, Lot 4G9
Persiaran Perdana, Precint 4
Federal Government Administrative Centre
62100 Putrajaya Federal Territory
Malaysia
Tel: 03-89115000 Fax: 03-89117959
Email: info@pdp.gov.my

PRAKATA

Tataamalan Umum Perlindungan Data Peribadi ini bertujuan untuk menguatkuasakan pematuhan kepada Seksyen 23 Akta Perlindungan Data Peribadi 2010 [Akta 709], peraturan-peraturan dan standard serta mewujudkan garis panduan kepada Golongan Pengguna Data yang tidak menyediakan Tataamalan dan tidak ada forum pengguna data untuk membangunkan Tataamalan yang berkaitan. Sekiranya memerlukan maklumat lanjut, sila rujuk —

Pesuruhjaya Perlindungan Data Peribadi di —

Aras 6, Kompleks KKMM, Lot 4G9
Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya, Malaysia
Tel: 03-8000 8000 | Faks: 03-8911 7959
E-mel: info@pdp.gov.my

TABLE OF CONTENTS

| NO. | DESCRIPTION | PAGE |
|------------|--|-------------|
| 1. | Introduction | 5 |
| 2. | Interpretation | 6 |
| 3. | General Principle (Section 6 of Act 709) | 9 |
| 4. | Notice and Choice Principle (Section 7 of Act 709) | 12 |
| 5. | Disclosure Principle (Section 8 of Act 709) | 17 |
| 6. | Security Principle (Section 9 of Act 709) | 19 |
| 7. | Retention Principle (Section 10 of Act 709) | 23 |
| 8. | Data Integrity Principle (Section 11 of Act 709) | 25 |
| 9. | Access Principle (Section 12 of Act 709) | 26 |
| 10. | <u>Rights of the Data Subject</u> | 27 |
| | i. Right of Access to Personal Data | 28 |
| | ii. Right to Correct Personal Data | 30 |
| | iii. Right to Withdraw Consent to Process Personal Data | 33 |
| | iv. Right to Prevent Processing Likely to Cause Damage or Distress | 33 |
| | v. Right to Prevent Processing for Purposes of Direct Marketing | 36 |
| 11. | General CoP of Personal Data Protection Compliance and Monitoring | 38 |
| 12. | Requirement of Preparing a CoP for the Specific Class of Data Users | 39 |
| 14. | Appendix 1: Personal Data Protection Notice | 40 |
| 16. | Appendix 2: Personal Data Access Request Form | 43 |
| 17. | Appendix 3: Personal Data Correction Request Form | 44 |
| 18. | Appendix 4: Notice under Subsection 43(1) of Act 709 | 47 |
| 19. | Appendix 5: List of Offences and Punishments under Act 709 and Subsidiary Legislation | 48 |

1. INTRODUCTION

1.1 Background

1.1.1 Pursuant to the Appointment of Date of Coming into Operation [*P.U. (B) 464/2013*], the Personal Data Protection Act 2010 [*Act 709*] came into operation on 15 November 2013. Under Act 709, a body who has been designated by the Personal Data Protection Commissioner as a data user forum in respect of a specific Class of Data Users may prepare a Code of Practice (CoP).

1.1.2 Section 24 of Act 709 provides for instances where the Personal Data Protection Commissioner may issue CoP. This General CoP of Personal Data Protection shall apply to the Class of Data Users who have not prepared a CoP and there is no data user forum to develop the relevant CoP for the Class of Data Users.

1.1.3 The objective of this General CoP of Personal Data Protection is to set out best practices for the data user to assist him in meeting the requirements under Act 709 when undertaking commercial transactions. The examples provided in this General CoP of Personal Data Protection are not intended to be exhaustive but are included for context and for the purposes of illustration. The recommendations provided in this General CoP of Personal Data Protection are good practices and the data user is encouraged to adopt these practices.

1.1.4 This General CoP of Personal Data Protection shall be read together with Act 709, regulations, actions, orders, directions, notifications, approvals, decisions and other executive acts howsoever called, made, given or done by the Personal Data Protection Commissioner.

1.2 **Non-compliance with this General CoP of Personal Data Protection**

1.2.1 This General CoP of Personal Data Protection has the force of law and is effective once it is registered by the Personal Data Protection Commissioner. As this General CoP of Personal Data Protection is legally binding, any data user who fails to comply with any provision of this General CoP of Personal Data Protection that is applicable to the data user commits an offence, and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both under Section 29 of Act 709.

2. **INTERPRETATION**

For the purpose of this General CoP of Personal Data Protection, the various words and terms used throughout this General CoP of Personal Data Protection shall have the same meaning as per Act 709, unless specified otherwise.

| Words | Meaning |
|-----------------------------|--|
| <i>personal data</i> | means any information in respect of commercial transactions, which — (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (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 |
| <i>sensitive personal data</i> | 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 belief or a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the <i>Gazette</i> |
| <i>vital interests</i> | means matters relating to life, death or security of a data subject |
| <i>use</i> | in relation to personal data, does not include the act of collecting or disclosing such personal data |
| <i>collect</i> | in relation to personal data, means an act by which such personal data enters into or comes under the control of a data user |
| <i>Minister</i> | means the Minister charged with the responsibility for the protection of personal data |
| <i>disclose</i> | in relation to personal data, means an act by which such personal data is made available by a data user |
| <i>relevant person</i> | in relation to a data subject, howsoever described, means — (a) in the case of a data subject who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the data subject; (b) in the case of a data subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorized in writing by the data subject to act on behalf of the data subject; or (c) in any other case, a person authorized in writing by the data subject to make a data access request, data correction request, or both such requests, on behalf of the data subject |
| <i>direct marketing</i> | means the communication by whatever means of any advertising or marketing material which is directed to particular individuals |

| | |
|----------------------------------|--|
| <i>correction</i> | in relation to personal data, includes amendment, variation, modification or deletion |
| <i>requestor</i> | in relation to a data access request or data correction request, means the data subject or the relevant person on behalf of the data subject, who has made the request |
| <i>data processor</i> | in relation to personal data, means 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 |
| <i>processing</i> | in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including — (a) the organization, adaptation or alteration of personal data; (b) the retrieval, consultation or use of personal data; (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of personal data |
| <i>data user</i> | means 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 personal data, but does not include a data processor |
| <i>relevant data user</i> | in relation to — (a) an inspection, means the data user who uses the personal data system which is the subject of the inspection; (b) a complaint, means the data user specified in the complaint; (c) an investigation — (i) in the case of an investigation initiated by a complaint, means the data user specified in the complaint; (ii) in any other case, means the data user who is the subject of the investigation; (d) an enforcement notice, means the data user on whom the enforcement notice is served |

| | |
|---------------------------------------|---|
| <i>third party</i> | in relation to personal data, means any person other than — (a) a data subject; (b) a relevant person in relation to a data subject; (c) a data user; (d) a data processor; or (e) a person authorized in writing by the data user to process the personal data under the direct control of the data user |
| <i>standard</i> | means a minimum requirement issued by the Commissioner, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context |
| <i>data subject</i> | means an individual who is the subject of the personal data |
| <i>commercial transactions</i> | means 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 |

3. **GENERAL PRINCIPLE (SECTION 6 OF ACT 709)**

3.1 The General Principle provides that —

- (a) the data user is required to obtain consent from the data subject prior to processing personal data unless the processing of personal data involves one of the following circumstances:
 - (i) for the performance of a contract to which the data subject is a party;
 - (ii) for the taking of steps at the request of the data subject with a view to entering into a contract;
 - (iii) for the compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
 - (iv) in order to protect the vital interests of the data subject;
 - (v) for the administration of justice; or

(vi) for the exercise of any functions conferred on any person by or under the law; and

(b) for processing of sensitive personal data, the data user is required to obtain explicit consent of the data subject.

3.2 The processing of personal data including sensitive personal data can only be performed if —

(a) the data subject has given his consent;

(b) personal data is processed for a lawful purpose;

(c) processing of personal data is necessary for or directly related to the purpose; and

(d) personal data collected is adequate, relevant and not excessive to the purpose for which personal data is processed.

3.3 **Consent of the data subject**

3.3.1 The data user shall obtain consent from the data subject in relation to the processing of personal data in any form that such consent can be recorded and maintained properly by the data user.¹ If the form in which such consent is to be given also concerns another matter, the requirement to obtain consent shall be presented distinguishable in its appearance from such other matter.

3.3.2 Consent for collecting, processing and disclosing the data subject's personal data can be obtained in several ways. Such consent provides the clearest indication that the data subject has consented to notify purposes of the collection, processing or disclosure of his personal data.

¹ Subregulation 3(1) of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

3.3.3 Example of forms of consent —

- (a) signature or clickable box indicating consent

☐ I hereby allow personal data processing rendered by me in this form for the purpose (s) _____ only.
(state the purpose)

Name:

Identity Card Number:

Example: *By clicking the “Agree” button through online application, it indicates that the data subject has provided consent for the processing of personal data.*

- (b) consent by conduct or performance: consent is considered as given by way of conduct or performance if —
- (i) the data subject does not object to the processing;
 - (ii) the data subject voluntarily discloses his personal data; or
 - (iii) the data subject proceeds to use the services of the data user; and

Example: *Consent is given by the data subject upon providing a copy of his identification document, whether or not it contains sensitive personal data to the data user.*

- (c) verbal consent: may be recorded either digitally (such as through the use of call logger and/or recorder software) or by issuing a written communication (such as issuing a letter, a form or an email from the data user’s official email) to the data subject confirming that consent has been given.

Example: Consent is given by a caller to the data user to process the caller's personal data when the caller calls the data user's customer service for their services.

3.3.4 The data user shall obtain consent from the parent, guardian or person who has parental responsibility on the data subject, if the data subject is under the age of eighteen (18) years.

3.3.5 The data user shall obtain consent from a person who is appointed by a court to manage the affairs of the data subject or a person authorized in writing by the data subject to act on his behalf if the data subject is incapable of managing his own affairs.

4. NOTICE AND CHOICE PRINCIPLE (SECTION 7 OF ACT 709)

4.1 The data user is required to make available a written notice, also known as a Personal Data Protection (PDP) Notice, to the data subject prior to or as soon as possible after the collection of his personal data. The PDP Notice is a written statement explaining how the data user processes personal data obtained from the data subject.

4.2 By examining the PDP Notice, the data subject should get a clear picture of how the data user will process personal data submitted and what options are available to the data subject. The PDP Notice should not be the platform for the data user to get the data subject's consent, especially a blanket consent. The data user has to obtain the consent in a proper method, to record and manage it accordingly.

4.3 When to give the PDP Notice

4.3.1 The PDP Notice shall be given as soon as practicable by the data user —

- (a) when the data subject is first asked by the data user to provide

his personal data;

- (b) when the data user first collects the personal data of the data subject;
- (c) before the data user uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or
- (d) before the data user discloses the personal data to a third party.

4.4 **Compulsory Elements**

4.4.1 The PDP Notice shall contain the following elements:

- (a) the processing of personal data
 - To name the details of personal data involved.
 - Type of personal data – to mention any sensitive personal data involved in processing.
 - To mention if the personal data of children under 18 years old are processed.
- (b) the need for processing
 - The purpose of processing.
 - To mention if there is any regulator requirement to collect certain personal data.
 - How long the personal data will be retained in such processing.
 - When will the personal data be disposed.
 - What practical measures will be taken to ensure personal data is secured.
- (c) the source of personal data
 - To mention all the relevant internal and external sources which refer to from where the personal data is obtained (e.g.: manual

or digital application/registration form).

(d) the rights of the data subject

- Personal data submission choice – compulsory or an option. If such personal data is compulsory, specify the consequences of not submitting it.
- How to access personal data submitted to the data user.
- How to correct or update the personal data.
- How to limit the processing of the personal data submitted - how to withdraw consent on personal data processing.
- How to contact data user for queries or complaints regarding personal data – to mention the name of person-in-charge, the designation, the contact number, and the e-mail address.

(e) the disclosure of personal data

- To name the third party to whom the personal data of data subject are shared with and for what purpose.
- To inform the security measures in place to ensure the disclosure implemented is safe and secure.

4.4.2 For the purposes of paragraph 7(1)(d) of Act 709, the data user shall provide the data subject the details as follows:

- (a) designation of the contact person;
- (b) phone number;
- (c) fax number, if any;
- (d) email address, if any; and
- (e) such other related information.²

² Regulation 4 of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

4.5 **Language**

4.5.1 The PDP Notice shall be in dual language; the national language and the English language. If there is any need to prepare the PDP Notice in other languages, the data user may do so.

4.6 **Method of Communication**

4.6.1 The data user may communicate the PDP Notice to the data subject by one or more of the following methods:

- (a) posting a printed copy of the PDP Notice to the last known address of the data subject based on the data user's record;
- (b) posting the PDP Notice on the website of the data user;
- (c) issuing a short message service (SMS) to the data subject with a website address/link to the PDP Notice and/or a telephone number in order to request for the PDP Notice and/or further information;
- (d) issuing an email to the data subject with a website address/link to the data user's PDP Notice and/or telephone number to contact for further information;
- (e) issuing an electronic message to the data subject providing a website address/link to the data user's PDP Notice and/or telephone number to contact for further information via such other electronic channels utilised by the data user;
- (f) inserting a summary notice in regular communications with the data subject (e.g. in monthly billing statements) with a website address/link to the PDP Notice and/or a telephone number to contact in order to request for the PDP Notice and/or further

information;

- (g) prominently displaying a summarised version of the PDP Notice at the premises of the data user's place of business (e.g. at the counter desk that the data subject comes to and/or at a prominent location in the data user's premises), and making available the full PDP Notice either upon a request being made at the counter to an employee of the data user;
- (h) displaying a message on the screens of kiosks with a website address/link to the PDP Notice, a telephone number to contact for further information and/or stating that the PDP Notice is available at the branch of the data user;
- (i) inserting a statement in application/registration forms referencing the PDP Notice, which may be accessed at a given website address/link, or by making a request to an employee of the data user, or by calling a telephone number provided in the application/registration form;
- (j) printing out copies of the PDP Notice and providing it to the data subject at the data user's premises; or
- (k) any other method of communication that serves to bring the PDP Notice to the data subject.

4.6.2 The data user shall determine the most appropriate method of communicating the PDP Notice which would reach as many of the data subjects as possible. It is recommended that the data user uses a variety of methods of communication to ensure that the PDP Notice is communicated as widely as possible.

4.6.3 The data user is required to maintain records of having communicated the PDP Notice to the data subject. This requirement may be fulfilled where the

data user maintains evidence or records that the PDP Notice has been communicated to the data subject.

4.6.4 The data user may refer to a sample template of the PDP Notice issued by the Personal Data Protection Commissioner appended as **Appendix 1**.

5. DISCLOSURE PRINCIPLE (SECTION 8 OF ACT 709)

5.1 The disclosure of the data subject's personal data is limited to the purpose and related purposes for which the original consent was obtained under the Notice and Choice Principle. The purpose declared by the data user for the collection of personal data in the PDP Notice is of importance as it effects whether additional consent needs to be obtained under the Disclosure Principle. The Disclosure Principle is closely related to the Notice and Choice Principle.

5.2 No personal data shall, without the consent of the data subject, be disclosed for any purpose other than —

- (a) the purpose for which the personal data was to be disclosed at the time of collection of personal data;
- (b) a purpose directly related to the original purposes; or
- (c) to any other party other than a third party of the class of third parties as specified in the PDP Notice.

5.3 Extent of further disclosure of personal data which falls outside the consent given by the data subject for the original purpose at the time collection is admissible. Such disclosure may be made under the following circumstances:³

- (a) the data subject has given his consent to the disclosure;

³ Section 39 Act 709

- (b) the disclosure —
 - (i) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or
 - (ii) was required or authorized by or under any law or by the order of a court;
- (c) the data user acted in the reasonable belief that he had in law the right to disclose the personal data to the other person;
- (d) the data user acted in the reasonable belief that 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
- (e) the disclosure was justified as being in the public interest in circumstances as determined by the Minister.

5.4 **List of disclosure**

5.4.1 The data user shall keep and maintain a list of disclosure to third parties for the purposes of paragraph 8(b) of Act 709 in relation to personal data of the subject data that has been or is being processed by him.⁴

5.5 **Disclosure to the data processor**

5.5.1 The data user is likely to disclose personal data to the data processor for various purposes relating to the data user's business. Where the data processor is engaged, it is recommended that the data user obtains warranties from the data processor in respect of the personal data to be disclosed. These warranties may include, among others —

- (a) that the data user shall only process personal data for purposes relating to his appointment by the data user, in

⁴ Regulation 5 of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

accordance with the data user's instructions, and no other purpose; and

- (b) the data processor shall comply with all applicable laws, regulations and industry standards relating to the privacy, confidentiality or security of the personal data.

6. SECURITY PRINCIPLE (SECTION 9 OF ACT 709)

6.1 The data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard —

- (a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;
- (b) to the place or location where the personal data is stored;
- (c) to any security measures incorporated into any equipment in which the personal data is stored;
- (d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
- (e) to the measure taken for ensuring the secure transfer of the personal data.⁵

6.2 The meaning of practical steps may vary from case to case, depending on the nature of personal data being processed by the data user and the degree of sensitivity attached to the personal data or the harm that the data subject might

⁵ Subsection 9(1) of Act 709

suffer due to its loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

6.3 Establishment of the security standard for personal data processed electronically

6.3.1 The data user shall, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard:⁶

| DATA SECURITY FOR PERSONAL DATA PROCESSED ELECTRONICALLY | |
|---|---|
| No. | Description |
| 1. | Register all employees involved in the processing of personal data. |
| 2. | Terminate an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organization. |
| 3. | Control and limit employee's access to personal data system for the purpose of collecting, processing and storing of personal data. |
| 4. | Provide user ID and password for authorized employees to access personal data. |
| 5. | Terminate user ID and password immediately when an employee who is authorized access to personal data is no longer handling the data. |
| 6. | Establish physical security procedures as follows: <ul style="list-style-type: none">i. control the movement in and out of the data storage site;ii. store personal data in an appropriate location which is unexposed and safe from physical or natural threats;iii. provide a closed-circuit camera at the data storage site (if necessary); andiv. provide a twenty four (24) hours security monitoring (if necessary). |
| 7. | Update the Back Up/Recovery System and anti-virus to prevent personal |

⁶ Part II, No. 4, Personal Data Protection Standard 2015

| | |
|-----|---|
| | data intrusion and such. |
| 8. | Safeguard the computer systems from malware threats to prevent attacks on personal data. |
| 9. | The transfer of personal data through removable media device and cloud computing service is not permitted unless with written consent by an officer authorized by the top management of the data user's organization. |
| 10. | Record any transfer of data through removable media device and cloud computing service. |
| 11. | Personal data transfer through cloud computing service must comply with the personal data protection principles in Malaysia, as well as with personal data protection laws of other countries. |
| 12. | Maintain a proper record of access to personal data periodically and make such record available for submission when directed by the Personal Data Protection Commissioner. |
| 13. | Ensure that all employees involved in processing personal data always protect the confidentiality of the data subject's personal data. |
| 14. | Bind an appointed third party by the data user with a contract for operating and carrying out personal data processing activities. This is to ensure the safety of personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. |

6.4 **Establishment of the security standard for personal data processed non-electronically**

6.4.1 The data user shall, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard:⁷

⁷ Part II, No. 5, Personal Data Protection Standard 2015

| DATA SECURITY FOR PERSONAL DATA PROCESSED NON-ELECTRONICALLY | |
|---|--|
| No. | Description |
| 1. | Register employees handling personal data into a system/registration book before being allowed access to personal data. |
| 2. | Terminate an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organization. |
| 3. | Control and limit employee's access to personal data system for the purpose of collecting, processing and storing of personal data. |
| 4. | Establish physical security procedures as follows: <ul style="list-style-type: none"> i. store all personal data orderly in files; ii. store all files containing personal data in a locked place; iii. keep all the related keys in a safe place; iv. provide record for keys storage; and v. store personal data in an appropriate location which is unexposed and safe from physical or natural threats. |
| 5. | Maintain a proper record of access to personal data periodically and make such record available for submission when directed by the Personal Data Protection Commissioner. |
| 6. | Ensure that all employees involved in processing personal data always protect the confidentiality of the data subject's personal data. |
| 7. | Record personal data transferred conventionally such as through mail, delivery, fax and etc. |
| 8. | Ensure that all used papers, printed documents or other documents exhibiting personal data are destroyed thoroughly and efficiently by using shredding machine or other appropriate methods. |
| 9. | Conduct awareness programmes to all employees (if necessary) on the responsibility to protect personal data. |

6.5 The data user shall ensure that the security standard in the processing of personal data be complied with by any data processor that carries out the processing

of the personal data on behalf of the data user.⁸ Where processing of personal data is carried out by the data processor on behalf of the data user, it is recommended that the data user uses reasonable efforts to include in his agreement with the data processor (whether in form of a contract, letter or any formal written document) —

- (a) provision on confidentiality, non-disclosure and technical and/or organizational security measures;
- (b) conditions under which personal data may be processed;
- (c) representations, undertakings, warranties and/or indemnities which are to be provided by the data processor;
- (d) security measures governing the processing to be carried out as may reasonably be contained in the data user's internal security policy and/or standards; and
- (e) deletion, destruction and/or return of personal data that is under the control of the data processor upon completion or termination of the contract or engagement, unless the user decides otherwise.

Example: *Security measures or controls should be implemented for high risk processing activities, may include but not limited to Robot Process Automation (RPA), artificial intelligence, data analysis and prospective emerging technologies.*

7. RETENTION PRINCIPLE (SECTION 10 OF ACT 709)

7.1 The Retention Principle restricts the data user from keeping personal data processed for any purpose longer than necessary for the fulfilment of the purpose. The data user may retain, keep or hold personal data of the data subject for as long as it is necessary to fulfil the purpose for which it was collected and in relation to the

⁸ Subregulation 6(3) of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

data user's business requirements provided that the retention is done according to the relevant legal and statutory requirements.

7.2 The provisions of other specific legislation concerning retention of personal data shall not be affected by the retention principle of Act 709 and such other applicable legislation shall be read together.

7.3 The standard for retention of personal data which is processed electronically and non-electronically

7.3.1 The data user 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 by having regard⁹ —

| No. | Description |
|-----|--|
| 1. | Determine the retention period in all legislation relating to the processing and retention of personal data are fulfilled before destroying the data. |
| 2. | Keep personal data no longer than necessary unless there are requirements by other legal provisions. |
| 3. | Maintain a proper record of personal data disposal periodically and make such record available for submission when directed by the Personal Data Protection Commissioner. |
| 4. | Dispose personal data collection forms used in commercial transactions within the period not exceeding fourteen (14) days, except if/unless the forms carry legal values in relation to the commercial transactions. |
| 5. | Review and dispose all unwanted personal data that in the database. |
| 6. | Prepare a personal data disposal schedule for inactive data with a twenty four (24) months period. The personal data disposal schedule should be maintained properly. |
| 7. | The use of removable media device for storing personal data is not permitted without written approval from the top management of the organization. |

⁹ Part II, No. 6, Personal Data Protection Standard 2015

7.4 Disposal of personal data

7.4.1 It shall be the duty of the data user 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 to be processed.¹⁰

7.4.2 Destruction is applicable to the paper based personal data and permanent deletion is applicable to the electronic personal data.

7.4.3 For personal data stored on an electronic medium, the permanent deletion of the personal data requires the electronic media (such as hard drive or a removable media device) to be wiped clean once the personal data has been deleted. The data user is to take reasonable effort to permanently delete the personal data from electronic media.

7.4.4 In the event of disposal, a disposal record should be kept to evidence the act of the disposal, *i.e.* by way of logbook, photographs or other methods that is relevant for record of disposal.

8. DATA INTEGRITY PRINCIPLE (SECTION 11 OF ACT 709)

8.1 Establishment of data integrity standard for personal data processed electronically and non-electronically

8.1.1 The data user shall 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 the personal data was collected and further processed. Such measures are:¹¹

¹⁰ Subsection 10(2) of Act 709

¹¹ Part II, No. 6, Personal Data Protection Standard 2015

| No. | Description |
|-----|--|
| 1. | Provide personal data update form for data subjects, either via online or conventional. |
| 2. | Update personal data immediately once data correction notice is received from data subject. |
| 3. | Ensure that all relevant legislation is fulfilled in determining the type of documents required to support the validity of the data subject's personal data. |
| 4. | Notify on personal data updates either through the portal or notice at premises or by other appropriate methods. |

8.2 What amounts to reasonable steps may differ from case to case, depending on the circumstances of each case as well as on the purpose and directly related purposes that the personal data was obtained for.

8.3 By way of illustration, Act 709 requires the data user to take reasonable steps to ensure that the personal data processed in relation to the data subject is —

- (a) accurate – meaning that the personal data is captured correctly;
- (b) complete – meaning that information in relation to the data subject has not been omitted;
- (c) not misleading – meaning that the personal data processed should not be ambiguous, deceiving or an oversight; and
- (d) kept up-to-date – meaning that the personal data of the data subject should reflect the latest verified information in respect of the data subject.

9. **ACCESS PRINCIPLE (SECTION 12 OF ACT 709)**

9.1 Access Principle requires the data user to give the data subject the right to access and correct his personal data which is inaccurate, incomplete, misleading or not up-to-date except where compliance with a request to such access or correction

is refused under Act 709.

9.2 **Compliance to the Access Principle**

9.2.1 In complying with the Access Principle, the data user shall observe the data subject's right to access the personal data and the right to correct the personal data in accordance with Act 709. The data user may refuse the right of the data subject to access and/or to correct his personal data provided that the refusal is in accordance with Act 709.

9.3 The maximum fees payable for a data access request by the data subject, as provided by the Personal Data Protection (Fees) Regulations 2013 [*P.U. (A) 338/2013*] are specified below¹² —

| Item | Description | Maximum fee (RM) |
|------|---|------------------|
| 1. | Data access request for a data subject's personal data with a copy | 10 |
| 2. | Data access request for a data subject's personal data without a copy | 2 |
| 3. | Data access request for a data subject's for a data subject's sensitive personal data with a copy | 30 |
| 4. | Data access request for a data subject's sensitive personal data without a copy | 5 |

10. **RIGHTS OF THE DATA SUBJECT**

10.1 Act 709 provides the data subject with the following rights:

- (a) right of access to personal data;
- (b) right to correct personal data;

¹² First Schedule, Regulation 2, Maximum Fees for Data Access Request, Personal Data Protection (Fees) Regulations 2013 [*P.U. (A) 338/2013*]

- (c) right to withdraw consent to process personal data;
- (d) right to prevent processing likely to cause damage or distress; and
- (e) right to prevent processing for purposes of direct marketing.

10.2 **Right of access to personal data**

10.2.1 The data subject is entitled to access his personal data which is being processed by or on behalf of the data user and has the right to lodge a Data Access Request (“DAR”) with the data user and to receive a reply from the data user within the time period provided in Act 709. For avoidance of doubt, personal data being retained for back up is not subject to be accessed by the data subject.

10.2.2 It is recommended that the data user provides a DAR form at suitable places and easy to obtain at the premises of the data user’s place of business when required by the data subject at the time of request. The data user may refer to a sample template of the DAR Form appended as **Appendix 2**.

10.2.3 **Compliance by the data user with the DAR**

The data user shall comply with the DAR by —

- (a) ensuring payment of the prescribed fees in accordance with the First Schedule of the Personal Data Protection (Fees) Regulations 2013 [*P.U. (A) 338/2013*] is made by the data subject. It is advised that the fees payable for the submission of the DAR to be stated in the DAR Form;
- (b) providing a standard form for request to access the personal data by the requestor;

- (c) providing the requestor a copy of the personal data of the data subject in any form as long as it can be comprehended by the requestor within twenty one (21) days from the date of receipt of the DAR;
- (d) if the data user is not able to comply with the DAR within the twenty (21) days' period, the data user is required to notify the requestor by notice in writing as to the reasons of his inability to do so and thereafter to comply with the valid DAR to the extent he is able to do so; and
- (e) complying in whole with the DAR not later than fourteen (14) days after the expiration of the twenty one (21) days' period.

10.2.4 **Refusal by the data user to comply with the DAR**

The data user has the right to refuse to comply with the DAR if —

- (a) inability to verify identity. The data user is not provided with necessary information as the data user may reasonable require in order to establish the identity of the data subject or where the DAR is submitted by the requestor, establish the requestor's connection to the data subject;
- (b) the data user is not provided with sufficient information to locate the personal data to which the data access request relates;
- (c) disproportionate burden. The burden or expense of providing access to personal data is disproportionate to the risk to the data subject's privacy for example if the time and cost to be incurred by the data user is greater than the significance of the personal data requested under the DAR;
- (d) disclosure of another. The data user is unable to comply with the DAR without disclosing another data subject's personal data. In

such a situation, the data user may either anonymise other data subject's personal data or seek consent from the data subject, or by any other practical means to disclose the personal data without breaching Act 709;

- (e) providing access would constitute a violation of an order of a court;
- (f) providing access would disclose confidential commercial information; or
- (g) such access to personal data is regulated by another law.

10.3 **Right to correct personal data**

10.3.1 The data subject is entitled to request personal data held by the data user be corrected if he is satisfied that the personal data is inaccurate, incomplete, misleading or not up-to-date by submitting a Data Correction Request ("DCR").

10.3.2 It is recommended that the data user provides a DCR Form at suitable places and easy to obtain at the premises of the data user's place of business when required by the data subject at the time of request. The data user may refer to a template of the DCR Form appended as **Appendix 3**.

10.3.3 **Validity of the DCR**

In ensuring that the DCR is valid, the data user is required to ensure that —

- (a) the DCR is made in writing;
- (b) the DCR is specific as to the personal data to be corrected;

- (c) the DCR contains the necessary information with certified documentation to establish the identity of the requestor and if the requestor is not the data subject, to establish the right and identity of the requestor and relationship of the requestor with the data subject;
- (d) the data user is supplied with such information as he may reasonably acquire to ascertain in what way the personal data to which the data correction relates is inaccurate, incomplete, misleading or not up-to-date;
- (e) the data user is satisfied that the personal data to which the data correction relates is inaccurate, incomplete, misleading or not up-to-date; and
- (f) the data user controls the processing of the personal data to which the data correction request relates and is not prohibited by another data user from complying with the data correction request.

10.3.4 **Compliance by the data user with the DCR**

The data user shall comply with the DCR not later than twenty one (21) days from the date of receipt of the DCR by —

- (a) making the necessary correction to the personal data;
- (b) supplying the requestor with a copy of the personal data as corrected;
- (c) taking all practicable steps to supply the third party with a copy of the corrected personal data accompanied by a notice in writing stating the reasons for the correction;

- (d) if the data user is unable to comply with a valid DCR within the twenty one (21) days' period from the date of receipt of the DCR, shall before the expiration of that period —
 - (i) inform the requestor by notice in writing that he is unable to comply with the DCR within such period and the reasons why he is unable to do so; and
 - (ii) comply with the DCR to the extent that he is able to do so; and
- (e) complying in whole with the DCR not later than fourteen (14) days after the expiration of the twenty one (21) days' period.

10.3.5 **Refusal by the data user to comply with the DCR**

The data user has the right to refuse to comply with the DCR if —

- (a) inability to verify identity. The data user is not provided with necessary information as the data user may reasonable require in order to establish the identity of the data subject or where the DCR is submitted by the requestor, establish the requestor's connection to the data subject;
- (b) inability to verify the need for correction. The data user is not supplied with sufficient information as the data user may reasonably require to determine how the personal data is inaccurate, incomplete, misleading or not up-to-date;
- (c) the data user is not satisfied that the personal data to which the DCR relates is inaccurate, incomplete, misleading or not up-to-date; or
- (d) the data user is not satisfied that the correction requested is accurate, complete, not misleading or up-to-date.

10.4 **Right to withdraw consent to the processing of personal data**

10.4.1 The 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.¹³

10.4.2 The data user shall, upon receiving the notice cease the processing of the personal data except to the extent where the withdrawal of consent would affect the data user's rights and obligations under contract or law. Example of such rights and obligations include —

- (a) the right to be paid for the services rendered, for example, the settlement of bookings or tax invoices or overdue payments;
- (b) the right to bring and maintain legal proceedings against the data subject;
- (c) the right to commence or continue with internal investigations involving the data subject;
- (d) the obligation to maintain personal data for such durations as required under applicable legislation; and
- (e) the conduct of internal audits, risk management and/or fulfilment of legal or regulatory reporting requirements.

10.5 **Right to prevent processing likely to cause damage or distress**

10.5.1 The data subject may, at any time by notice in writing to the data user, require the data user to —

- (a) cease processing the personal data; or

¹³ Subsection 38(1) of Act 709

- (b) not begin the personal data processing,

where the processing is causing or is likely to cause substantial and unwarranted damage or distress to the data subject or another person.

10.5.2 **Requirement**

The data subject is required to prove that —

- (a) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another person; and
- (b) the damage or distress is or would be unwarranted.

In most cases —

- (a) “substantial damage” includes financial loss suffered by the data subject or another person;
- (b) “substantial distress” includes emotional or mental trauma suffered by the data subject or another person; and
- (c) “unwarranted” means that the damage or distress suffered by the data subject or another person is not justifiable.

10.5.3 **Circumstances where the data subject does not have the right to prevent processing**

The data subject shall not have the right to prevent processing where —

- (a) the data subject has consented to the processing; or
- (b) the processing of personal data is necessary —
 - (i) for the performance of a contract to which the data subject is a party;
 - (ii) for the taking of steps at the request of the data subject with a view to entering into a contract;
 - (iii) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by contract; or
 - (iv) in order to protect the vital interests of the data subject.

10.5.4 Compliance by the data user with the right to prevent processing likely to cause damage or distress

Upon receiving a written notice to cease processing or not to commence processing of personal data, the data user shall, within twenty one (21) days, provide the data subject a written notice stating —

- (a) that the data user has complied or intends to comply with the data subject notice;
- (b) if the data user does not intend to comply with the data subject notice, to provide reasons for the decision; or
- (c) stating reasons why the data user finds the data subject notice unjustified or to any extent unjustified and the extent to which the data user has complied or intends to comply (if any).

The data user may consider the following when making a decision on whether to comply with the request —

- (a) are there legitimate reasons for the data subject's request? The data subject should provide legitimate reasons as the damage or distress caused shall be substantial; and

- (b) is the damage or distress unwarranted? This is tied to whether the data subject has provided legitimate reasons for the request.

Where the data user does not comply with the notice, the data subject may apply to the Personal Data Protection Commissioner to require the data user to comply with the notice. If the Personal Data Protection Commissioner is satisfied that the data subject's request is justified, the Personal Data Protection Commissioner may require the data user to comply with the request.

10.6 **Right to Prevent Processing for Purposes of Direct Marketing**

10.6.1 Pursuant to Act 709, the data subject has the right at any time, by notice in writing to the data user, to require the data user to either cease or not begin processing his personal data for purposes of direct marketing. The data user may refer to a sample template of the notice under Subsection 43(1) of Act 709 appended as **Appendix 4**.

10.6.2 The data user shall comply with such a request within a reasonable time frame.

10.6.3 The data user who is communicating advertising or marketing materials directed to a particular data subject, through the utilisation of the data subject's personal data, is required to either has already notified the data subject via his PDP Notice, or in cases where the PDP Notice is silent as to the issuance of such advertising or marketing materials, is required to obtain the consent of the data subject prior to commencing direct marketing.

10.6.4 The data user is permitted to conduct direct marketing to the data subject —

- (a) if consent is obtained from the data subject;

- (b) for the collection of personal data for sale of products or provision of services;
- (c) if the data subject is informed of the identity of direct marketing organisations and the purpose of collection and disclosure;
- (d) in the event the product and/or services offered to the data subject are similar to the product and services generally provided by the data user;
or
- (e) in the event the data user is committed to providing an opt-out option for the data subject during the collection of personal data.

10.6.5 Where the data subject makes a written request asking to receive some direct marketing materials and not others, the data user may choose not to provide the data subject with all direct marketing materials, should his system be incapable of distinguishing between the different types of direct marketing materials.

10.6.6 If the data subject is dissatisfied with the failure of the data user to comply in whole or in part with the written request, the data subject may submit an application to the Personal Data Protection Commissioner to require the data user to comply. Failure by the data user to comply with the requirement of the Personal Data Protection Commissioner constitutes an offence liable to punishment with a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two (2) years or to both.

11. GENERAL CoP OF PERSONAL DATA PROTECTION COMPLIANCE AND MONITORING

11.1 The data user is required to maintain a personal data system. The personal data system shall at all reasonable times be open to the inspection of the Personal Data Protection Commissioner or any inspection officer.¹⁴

11.2 The data user shall maintain —

- (a) in relation to the General Principle, the record of the consent from the data subject maintained in respect of the processing of personal data by the data user;
- (b) in relation to the Notice and Choice Principle, the record of a written notice issued by the data user to the data subject in accordance with Section 7 of Act 709;
- (c) in relation to the Disclosure Principle, the list of disclosure to third parties for the purposes of paragraph 8(b) of Act 709 in respect of personal data that has been or is being processed by him;
- (d) in relation to the Security Principle, the security policy developed and implemented by the data user for the purposes of Section 9 of Act 709;
- (e) in relation to the Retention Principle, the record of compliance in accordance with the retention standard;
- (f) in relation to the Data Integrity Principle, the record of compliance in accordance with the data integrity standard; or
- (g) such other related information which the Personal Data Protection Commissioner or any inspection officer deems necessary.

¹⁴ Subregulation 14(1) of the Personal Data Protection Regulations 2013 [*P.U. (A) 335/2013*]

11.3 The data user is required to develop and implement appropriate compliance policies and procedures (compliance framework) in order to ensure compliance with this General CoP of Personal Data Protection, Act 709, regulations and standard.

11.4 It is recommended that the data user continuously monitor his compliance with this General CoP of Personal Data Protection, Act 709, regulations and standard by —

- (a) implementing an internal monitoring framework; and
- (b) conducting self-audits.

11.5 The data user is encouraged to ensure that appropriate training and/or awareness is put in place for employees to ensure that employees understand the importance of complying with these policies and procedures. Relevant employees may be identified to receive specific training, such as training on security and fraud awareness and on handling data access/correction requests.

11.6 The data user is required to ensure that he keeps up with the latest developments in Act 709 and continue to provide training to employees as and when required to keep up with any changes.

12. REQUIREMENT OF PREPARING A COP FOR THE SPECIFIC CLASS OF DATA USERS

12.1 A body who has been designated by the Personal Data Protection Commissioner as a data user forum in respect of a specific class of data shall prepare a CoP for the specific class of data users within two (2) years from the date of the designation.

12.2 The Personal Data Protection Commissioner may revoke, amend or revise, whether in whole or in part, any CoP registered under Act 709 by virtue of Section 26 of Act 709.

Appendix 1

Personal Data Protection Notice

[Logo / Organisation name]

(Effective date: dd mm yy)

(Last reviewed: dd mm yy)

INTRODUCTION

(Insert organisation name) care about your personal data protection. This notice clarifies how (your business name) processes your data from the point we collect, use, share, dispose of and the security measures that we established to ensure your personal data is well protected.

COLLECTION OF PERSONAL DATA

We collect your personal data which range from your name, home address, email address, phone number and your bank account. [Change / add to this list as appropriate]

SOURCE OF PERSONAL DATA COLLECTION

We gather your personal data from:

1. New member registration form available at our website (your website address)
2. Purchase form
3. Cookies
4. [Change / add to this list as appropriate]

REASON FOR PERSONAL DATA COLLECTION

We collect your personal data to:

1. Process your request to purchase our product / service
2. Deliver our product to your desired address and location
3. Resolve complaint / delivery problem (if any)
4. Send new product promotion to you (only with your consent)
5. [Change / add to this list as appropriate]

PROCESSING OF PERSONAL DATA

We only process your personal data within Malaysia. Your personal data will not be transferred to any place outside Malaysia. **[Change as appropriate]**

DISCLOSURE OF PERSONAL DATA

We disclose your personal data to:

1. The appointed courier to deliver your purchased product
2. The authority for legal / regulatory purpose **(name the parties involved)**
3. **[Change / add to this list as appropriate]**

SECURITY MEASURE

We take these measures to protect your personal data:

1. By ensuring your personal data is kept as required by Act 709
2. By ensuring our staff not to misuse your personal data
3. By performing contract / agreement with system vendor, appointed courier company.
4. **[Change / add to this list as appropriate]**

Nevertheless, you are required to ensure the security of your password and not to disclose it to another party to reduce the risk of data breaches.

PERSONAL DATA RETENTION PERIOD

We will retain your personal data for seven (7) years / as long as you are our customer **[Change as appropriate]**. If you are no longer our customer, we will permanently delete your personal data.

YOUR RIGHTS

You have the rights to:

1. Correct / update your personal data **(insert the link to the form available)**
2. Access your personal data which we process and keep with us
3. Stop any of our new promotional products sent to you
4. Withdraw your consent for us to process your personal data **[Inform the consequences]**.

CONTACT US

You can contact us or submit your inquiry in regards to the processing of your personal data at:

(Name)

(Designation)

(Address)

(Telephone number)

(Fax number / email address)

Appendix 2

PERSONAL DATA PROTECTION ACT 2010 [ACT 709] PERSONAL DATA ACCESS REQUEST FORM

The following information is required to help us provide you a timely and accurate response to your Personal Data Access Request pursuant to Act 709.

| | |
|--|--|
| Full Name of Data Subject or Relevant Person | |
| Relevant Person's Relationship with the Data Subject | |
| Address | |
| Mobile Number | |
| Email address | |
| <p>Please provide details of the information you require from [Data User]:</p> | |

Declaration: I am the Data Subject/Relevant Person named above and hereby request, under the provisions of Sections 12 and 30 of the Personal Data Protection Act 2010 [Act 709], that [**Data User**] provide me with a copy of the personal data held about me as specified above. I understand that there may be a charge for this service and that [**Data User**] will contact me to request payment. I also note that the [**Data User**] will respond within the time stipulated under Act 709 after receipt of payment from me and will notify me of a date and time to collect a copy of the documents personally.

Signature

Date

Appendix 3

| PERSONAL DATA CORRECTION REQUEST FORM | |
|--|--|
| <ul style="list-style-type: none">• Please note that we reserve the right to restrict and/ or refuse your access to certain particulars of your personal data as may be permitted under the Personal Data Protection Act 2010 [Act 709].• Your request may not be processed if the information/document provided is incomplete.• Any request for Personal Data Correction Request must be supported with proof or evidence.• Please use CAPITAL LETTERS to fill in the form. | |
| Please tick (✓) on one of the following: <ul style="list-style-type: none"><input type="checkbox"/> I would like to access my personal data (Please fill in Section 1 and Section 3 below)<input type="checkbox"/> I am a Third Party Requestor (Please fill in Section 2 and Section 3 below) | |
| SECTION 1 : TO BE FILLED IN BY DATA SUBJECT | |
| Full Name (per NRIC/Passport) | |
| New NRIC/Passport No. | |
| Mobile Phone No. | |
| SECTION 2: TO BE FILLED IN BY THIRD PARTY REQUESTOR (AUTHORIZED PERSON) | |
| This request is based on (please tick (✓) one of the following): <ul style="list-style-type: none"><input type="checkbox"/> I am acting under the Data Subject's authorisation/mandate/Power of Attorney<input type="checkbox"/> I am the legal/personal representative of the Data Subject<input type="checkbox"/> I have Warrant or Court Order allowing the correction to the Data Subject's Personal Data<input type="checkbox"/> I am executor/administrator of the Data Subject's estate<input type="checkbox"/> Others (please specify) _____ | |
| Please enclose proof of your authority to correct the personal data of the Data subject. | |
| A : Particulars of Data Subject | |
| Full Name (per NRIC/Passport) | |

| | |
|---|---|
| New NRIC/Passport No. | |
| Mobile Phone | |
| B: Particulars of Third Party Requestor | |
| Full Name (per NRIC/Passport) | |
| New NRIC/Passport No. | |
| Mobile Phone | |
| Email Address | |
| Correspondence Address | |
| SECTION 3 : CORRECTION OF PERSONAL DATA | |
| (Please tick (√) and fill in at relevant Section only) | |
| <input type="checkbox"/> Full Name (per NRIC/Passport) | |
| <input type="checkbox"/> New NRIC/Passport No. | |
| <input type="checkbox"/> Address of premise | |
| <input type="checkbox"/> Mobile Phone | |
| <input type="checkbox"/> Postal Address | |
| <input type="checkbox"/> *House Phone No. | |
| <input type="checkbox"/> *Office Phone No. | |
| <i>*Non-mandatory information</i> | |
| DECLARATION | |
| Declaration by the Data Subject I, declare that I am the person named in Section 1 and I am requesting to correct my own personal data. I confirm that the information supplied in this form is true and accurate. | Declaration by the Third Party Requestor I, declare that I am the Authorized Person named in Section 2 and I am requesting to correct the Data Subject's personal data. I confirm that the information supplied in this form is true and accurate. |

Appendix 4
NOTICE UNDER SUBSECTION 43(1) OF
THE PERSONAL DATA PROTECTION ACT 2010 [ACT 709]

Date:

Data User's Address:

.....
.....
.....

Sir / Madam,

NOTICE UNDER SUBSECTION 43(1) OF THE PERSONAL DATA PROTECTION
ACT 2010 [ACT 709] TO PREVENT PROCESSING OF PERSONAL DATA FOR
PURPOSES OF DIRECT MARKETING

I, (full name)
(New NRIC/Passport No.) need you to cease or not to begin processing my personal
data for purposes of direct marketing in the duration of _____ *
from the date of receipt of this notice.

Thank you.

Signature:

Name:

Address:

.....
.....
.....

Phone No.:

Email:

*Data subject can determine a reasonable stipulated time

Appendix 5

LIST OF OFFENCES AND PUNISHMENTS UNDER THE PERSONAL DATA PROTECTION ACT 2010 [ACT 709] AND SUBSIDIARY LEGISLATION

| ITEM | SECTION / REGULATION | OFFENCE | PUNISHMENT |
|-------------|---|---|--|
| 1. | Subsection 5(2) Personal Data Protection Principles | Non-compliance with data processing under the Personal Data Protection Principles | Fine not exceeding RM300,000 or imprisonment for a term not exceeding two (2) years or both |
| 2. | Subsection 16(4) Certificate of registration | Process personal data without certificate of registration issued in paragraph 16(1)(a) | Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both |
| 3. | Subsection 18(4) Revocation of registration | Process personal data after registration is revoked | Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both |
| 4. | Subsection 19(2) Surrender of certificate of registration | Failure to surrender the certificate of registration to the Personal Data Protection Commissioner after it is revoked | Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both |
| 5. | Section 29 Non-compliance with the CoP | Non-compliance with any provision of the CoP that is applicable to the data user | Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both |
| 6. | Subsection 37(4) Notification of refusal to comply with data correction request | Non-compliance with any provision in subsection 37(2) | Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both |
| 7. | Subsection 38(4) | Continue to process | Fine not exceeding |

| | | | |
|-----|--|--|---|
| | Withdrawal of consent to process personal data | personal data after withdrawal of consent by the data subject | RM100,000 or imprisonment for a term not exceeding one (1) year or both |
| 8. | Subsection 40(3) Processing of sensitive personal data | Processing sensitive personal data without complying with the conditions in subsection 40(1) | Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both |
| 9. | Subsection 42(6) Right to prevent processing likely to cause damage or distress | Non-compliance with the Personal Data Protection Commissioner's requirements in subsection 42(5) | Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both |
| 10. | Subsection 43(4) Right to prevent processing for purposes of direct marketing | Non-compliance with the Personal Data Protection Commissioner's requirements in subsection 43(3) | Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both |
| 11. | Subsection 108(8) Enforcement notice | Non-compliance with an enforcement notice | Fine not exceeding RM200,000 or imprisonment for a term not exceeding two (2) years or both |
| 12. | Subsection 113(7) Search and seizure with warrant | A person who without lawful authority, breaks, tampers with or damages the seal referred to in subsection 113(6) or removes any computer, book, account, computerised data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article under seal or attempts to do so | Fine not exceeding RM50,000 or imprisonment for a term not exceeding six (6) months or both |

| | | | |
|-----|---|---|---|
| 13. | Section 120 Obstruction to search | Any person who — (a) refuses to give access to any authorized officer; (b) assaults, obstructs, hinders or delays any authorized officer; or (c) refuses any authorized officer any information relating to an offence or suspected offence | Imprisonment for a term not exceeding two (2) years or fine not exceeding RM10,000 or both |
| 14. | Subsection 129(5) Transfer of personal data to places outside Malaysia | Non-compliance with requirements in subsection 129(1) — transfer personal data of a data subject to a place outside Malaysia unless to such a place as specified by the Minister, upon the recommendation of Personal Data Protection Commissioner, by notification published in the <i>Gazette</i> | Fine not exceeding RM300,000 or imprisonment for a term not exceeding two (2) years or both |
| 15. | Subsection 130(7) Unlawful collecting, etc., of personal data | Committing offences as prescribed in section 130 | Fine not exceeding RM500,000 or imprisonment for a term not exceeding three (3) years or both |
| 16. | Subsection 131(1) and (2) Abetment and attempt punishable as offences | Subsection 131(1) Abetment of a commission of or attempts to commit any offence under Act 709 | Provided that any term of imprisonment shall not exceed half of the maximum term provided for the offence under Act 709 |

| | | | |
|---|---|---|---|
| | | Subsection 131(2) Commission of any act preparatory to or in furtherance of the commission of any offence under Act 709 | Provided that any term of imprisonment shall not exceed half of the maximum term provided for the offence under Act 709 |
| 17. | Subsection 141(2) Obligation of secrecy | Offence under paragraphs 141(1)(a) and (b) — the Personal Data Protection Commissioner, its officer or servant, any member of the Advisory Committee, any member, officer or servant of the Appeal Tribunal, any authorized officer or any person attending any meeting or deliberation of the Advisory Committee, whether during or after his tenure of office or employment, at any time shall not disclose any information obtained by him in the course of his duties | Fine not exceeding RM100,000 or imprisonment for a term not exceeding one (1) year or both |
| 18. | Subsection 143(3) Power to make regulation | Non-compliance with any regulation or any other subsidiary legislation under this section | Fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both |
| <p style="text-align: center;">PERSONAL DATA PROTECTION REGULATIONS 2013 [P.U. (A) 335/2013]</p> | | | |
| 1. | Regulation 12 Penalty | Non-compliance with the following: | Fine not exceeding RM250,000 or imprisonment |

| | | | |
|--|--|--|--|
| | | <ul style="list-style-type: none"> • subregulation 3(1) consent of data subject • regulation 6 security policy • regulation 7 retention standard • regulation 8 • data integrity standard | for a term not exceeding two (2) years or both |
|--|--|--|--|

**PERSONAL DATA PROTECTION (REGISTRATION OF DATA USER)
REGULATIONS 2013 [P.U. (A) 337/2013]**

| | | | |
|----|--|---|--|
| 1. | Regulation 5 Renewal of certificate of registration | Failure to renew certificate of registration | Fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both |
| 2. | Regulation 6 Change of particulars in certificate of registration | Failure to notify the commissioner of any change to the particulars of certificate of registration | Fine not exceeding RM250,000 or imprisonment for a term not exceeding two (2) years or both |
| 3. | Regulation 8 Display of certificate of registration and other information | Failure to display certificate of registration and other information | Fine not exceeding RM10,000 or imprisonment for a term not exceeding one (1) year or both |