THE PERSONAL DATA PROTECTION CODE OF PRACTICE

For Licensees Under The Communications And Multimedia Act 1998

March 2015

Table Of Contents

PART 1
INTRODUCTION

1.0 Foreword

1.1 The Personal Data Protection Act 2010 ("the Act") was passed by the Parliament of Malaysia for the purpose of regulating the processing of personal data in commercial transactions. The Act came into force on 15 November 2013. The Act confers rights on individuals ("Data Subjects") in relation to the collection, use and/or retention ("processing") of their personal data, and places obligations on those persons/entities processing the same ("Data Users"). The terms "Data Subject", "Data User" and "processing" are more fully defined in Part 2 of this Code of Practice.

1.2 The Act is built around a core of personal data protection principles which state in broad terms the types of conduct that are permitted under the Act.

1.3 In recognition of the fact that separate sectors/industries may have specific industry practices in relation to the manner in which personal data is handled and/or may have deployed unique technologies which require specific data protection rules, the Act permits the formation and designation by the Commissioner of data user forums, and the preparation of codes of practice for specific industries/sectors.

1.4 This Code of Practice is specific to the persons/parties that hold licences under the Communications and Multimedia Act 1998, and has been developed by the Personal Data User Forum for Communications and Multimedia Act Licensees ("CMA Data User Forum"). For the avoidance of doubt, this Code applies to both individual and class licensees under the Communications and Multimedia Act 1998, but does not extend to those parties that have been exempted from holding a licence under the Communications and Multimedia Act 1998 and its regulations.

2.0 Objectives of the Code

2.1 This Code of Practice ("Code") is intended to:-

(i) set standards of conduct in respect of personal data that are expected of a particular class of Data Users (as defined in Part 2), namely individual and class licensees under the Communications and Multimedia Act 1998;

(ii) serve as a guide to Data Users in order to ensure that the processing of personal data does not infringe a Data Subject's (as defined in Part 2) rights under the Act; and

(iii) serve as a guide to Data Users to set effective standards and measures in relation to the processing of a Data Subject's personal data.

3.0 Scope of the Code

3.1 Upon registration of this Code by the Commissioner, the Code shall apply to all Data Users. This shall include all:

(i) Network Facilities Providers;
(ii) Network Services Providers;
(iii) Applications Service Providers; and
(iv) Content Applications Service Providers,

as defined in the Communications and Multimedia Act 1998.

3.2 This Code shall apply to the following relationships in which Data Users process the personal data of individuals:-

(i) ***Relationship between Data User and Individuals***

This Code shall apply to the relationship between Data Users and individuals, including but not limited to:-

- individuals who are (or were) customers of Data Users;
- individuals that represent customers of Data Users (e.g. parents of minors, trustees and authorised representatives);
- individuals that have been identified as potential customers of Data Users;
- individuals that have applied to be customers of a Data User, whether successfully or otherwise; and
- individuals that have entered into ancillary arrangements with a Data User (e.g. guarantors and/or third party security providers) on behalf of another individual or entity.

(ii) ***Relationship between Data User and Third Party Service Provider***

This Code shall apply to the relationship between Data Users and third party service providers ("data processors"), for example, where the Data User outsources certain functions (e.g. marketing, debt collection) to third parties and provides the said third parties with the relevant personal data of customers (Data Subjects inclusive).

(iii) ***Relationship between the Data User and Personnel***

This Code shall apply to the relationship between Data Users and their personnel, but only to the extent that it involves the processing of personal data of Data Subjects by the personnel of the Data Users.

3.3 In so far as organizations / companies, the information of their officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, suppliers/vendors and/or related parties are provided by the said organizations/companies to Data Users for the purpose of securing subscription accounts or such other facilities from the said Data Users, the said information shall be treated as information that the said organization / company is authorised to provide to the Data User.

3.4 For the avoidance of doubt, Data Users are not required to obtain consent from the said officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, suppliers/vendors and/or related parties, in order to process said information for the purpose of the organization / company securing subscription accounts or such other facilities or products from the said Data Users.

3.5 Other than the above, this Code shall apply to personal data that is:

(i) collected, used, retained and/or deleted, whether automatically or otherwise, via the use of electronic devices, including but not limited to computers, servers, mobile phones, USB thumb drives; and/or

(ii) collected and recorded as part of a manual filing system ("relevant filing system") or with the intention that it should form part of the said manual filing system. Examples of this would include a physical filing system where Data Subjects are identified alphabetically or through some other identifier.

3.6 This Code shall apply to all personal data and sensitive personal data that is in the possession or under the control of Data Users, irrespective as to the date of the said personal data / sensitive personal data being collected or otherwise "processed".

3.7 For the avoidance of doubt, deceased individuals are not recognised by the Commissioner as Data Subjects under the Act, Regulations and this Code.

4.0 Code Administration

4.1 The CMA Data User Forum shall administer this Code as may be stipulated by the Commissioner.

4.2 The Commissioner may, upon an application by the CMA Data User Forum, revoke, amend or revise this Code, whether in whole or in part.

4.3 The Commissioner and the CMA Data User Forum shall meet at least once annually in order to discuss issues relating to compliance with the Act by Data Users, enforcement actions under the Act, complaints lodged against Data Users, proposed initiatives of the Commissioner and any other relevant matter.

5.0 Acceptance of The Code by The Commissioner

5.1 This Code has been accepted by the Commissioner pursuant to section 23(4) of the Act, wherein:-

(i) the Code is consistent with the provisions of the Act;
(ii) the purpose for the processing of personal data by Data Users has been taken into consideration;
(iii) the views of the Data Subjects or groups representing Data Subjects have been taken into consideration;
(iv) the views of the Communications and Multimedia Commission of Malaysia having been taken into consideration; and
(v) the Code offers an adequate level of protection for the personal data of the Data Subjects concerned.

6.0 Effective Date

6.1 Pursuant to section 23(4) of the Act, this Code shall only be effective upon registration of the Code by the Commissioner in the Register of Codes of Practice ("Effective Date").

6.2 Data Users shall be given a grace period of six (6) months from the Effective Date to comply with this Code.

7.0 Legal Force and Effect of The Code

7.1 All Data Users dealing with personal data are bound to comply with this Code by virtue of section 25 of the Act.

7.2 A Data User that fails to comply with any provision of this Code 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 as stipulated in section 29 of the Act.

7.3 Compliance with this Code shall be a defence against any action, proceeding or prosecution, brought against a Data User, whether in court or otherwise, for one or more alleged breaches of the Act and/or the Regulations.

PART 2
DEFINITIONS

1.0 Definitions

For the purpose of this Code, the various words and terms used throughout this Code shall have the same meaning as in the Act, unless specified otherwise.

Applications Service	means a service provided by means of, but not solely by means of, one or more network services;
Application Service Provider	means a person who provides an Applications Service;
CMA Data User Forum	refers to the Personal Data User Forum For Communications and Multimedia Act Licensees as established pursuant to section 21 of the Act;
Code	means this Code of Practice as may be revised from time to time;
Code of Practice	means the personal data protection code of practice in respect of the licensees under the Communications and Multimedia Act 1998, as registered by the Commissioner pursuant to section 23 of the Act;
Collect	means in relation to personal data, an act by which personal data enters into or comes under the control of a Data User;
Commercial transaction	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;
Commissioner	means the Personal Data Protection Commissioner appointed pursuant to the Act;
Content Application Service Provider	means a person who provides Applications Service which provides content (any sound, text, still picture or other audio-visual representation, tactile representation or any combination of the preceding which is capable of being

	created, manipulated, stored, retrieved or communicated electronically);
Data processor	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;
Data Subject	means an individual who is the subject of personal data and for the purposes of this Code includes (without limitation) the individuals identified in 3.2 of Part 1;
Data User	means a licensee, whether class or individual, under the Communications and Multimedia Act 1998 who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data (but does not include a data processor), and for the purpose of this Code shall also refer to the persons that are subject to the Code;
Defaulters Database	means a database containing a list of customers absconding without payment/defaulting in payments for services rendered by Data Users;
Disclose	in relation to personal data, means an act by which such personal data is made available by a Data User;
Individual	means a living human being, separate and distinct from companies or other corporate entities;
Network Facilities	means any element or combination of elements of physical infrastructure used principally for, or in connection with, the provision of Network Services, but does not include customer equipment;
Network Facilities Provider	means a person who owns or provides any Network Facilities;
Network Service	means a service for carrying communications by means of guided and/or unguided electromagnetic radiation;
Network Services Provider	means a person who provides Network Services;

Personal data	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;
Processing / process	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;
Privacy Notice	means the notice in writing that a Data User is required to provide to a Data Subject in compliance with section 7 of the Act, as may be amended by the said Data User from time to time;
Regulations	refers to the regulations made by the Minister pursuant to section 143(1) of the Personal Data Protection Act 2010;

Relevant filing system	means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set of information is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;
Sensitive personal data	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 that the Minister may determine by order published in the Gazette;
Subscriber	means an individual who has entered into a contract with the Data User for the supply of products and/or services;
The Act	means the Personal Data Protection Act 2010 and includes all modifications and amendments thereto and the accompanying regulations;
Third party	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; and
Writing / written	includes type writing, printing, lithography photography, electronic storage or transmission or any other method of recording information or fixing information in a form capable of being preserved.

2.0 INTERPRETATION

2.1 For the purpose of this Code:

(i) the singular includes the plural and vice versa except where the context otherwise requires;
(ii) references to "includes" or "including" are to be construed without limitation;
(iii) references to “person” or “persons”, are to be read to include parties in the form of entities; and
(iv) references to any statute include reference to every order, instrument, regulation, direction or plan having the force of law made thereunder or deriving validity therefrom and any amendment or re-enactment of the same from time to time in force.

2.2 Examples provided in this Code are not intended to be exhaustive but are included for context and illustration purposes only.

2.3 Recommendations provided in this Code are not mandatory and merely serve as a guide on good practice that Data Users are encouraged to adopt.

PART 3
GENERAL PRINCIPLES APPLICABLE TO THE DATA USER AND DATA SUBJECT RELATIONSHIP

1.0 GENERAL PRINCIPLE

Consent

1.1 Data Users are permitted to *"process"* (e.g. to collect, use, modify, store and/or dispose of) personal data, either with or without consent, as detailed in 1.2 and 1.3 below.

1.2 Data Users are permitted to process personal data without obtaining the consent of Data Subjects where the processing is necessary for the following purposes:

(i) the performance of a contract entered into with a Data Subject; or
(ii) the fulfilment of a pre-contractual inquiry of a Data Subject who is a potential customer; or
(iii) in order to comply with any non-contractual legal obligation that the Data User is subject to; or
(iv) in order to protect the vital interests of the Data Subject- (e.g. disclosing the last known location of the Data Subject where he/she has been reported missing for more than 24 hours); or
(v) for the administration of justice in accordance with the requirements and processes as set out by law; or
(vi) for the exercise of any functions conferred upon any person by the law

1.3 In all other circumstances, Data Users are required by the Act to obtain the consent of the Data Subject before *"processing"* the said personal data.

Form And Type Of Consent

1.4 Where consent needs to be obtained from Data Subjects, the form and type of consent that needs to be obtained prior to processing personal data has not been specified in the Act. However, the Regulations provide that consent needs to be capable of being *"recorded"* and *"maintained"*. As such, subject to the foregoing, consent may be express or implied.

1.5 Examples of forms of consent acceptable under the Act for the purpose of commencing or continuing a contract between the Data User and the Data Subject are:

(i) signatures or ticks indicating consent; or
(ii) opt-in consent; or
(iii) deemed consent ; or

(iv) verbal consent; or
(v) consent by conduct/performance,

subject to fulfilment of the requirements of the Regulations as to consent being capable of being *"recorded"* and *"maintained"*.

1.6 Subject to compliance with the Notice and Choice principle as addressed in 2.0 below, "deemed consent" means where consent can be understood to have been given by the Data Subject to the Data User in instances where the Data Subject:

(i) does not object to the Data User processing his/her personal data; or
(ii) proceeds to volunteer his/her personal data; or
(iii) proceeds to use the services of the Data User; or
(iv) continues to use the services being subscribed to.

1.7 In situations where a Data Subject fails to respond to a request for consent or where it may be difficult to secure the consent of the Data Subject (e.g. where the Data Subject has defaulted in payment or is not contactable), the Data User is required to demonstrate that reasonable steps were taken to obtain the consent of the Data Subject.

1.8 Where applicable, consent may be obtained either on paper or on electronic mediums utilised by Data Users including but not limited to electronic channels such as SMS, e-mail and other internet / social / application based messaging systems.

1.9 It is recommended that where verbal consent is being recorded, the said consent will need to be recorded either digitally (e.g. via the use of call logger and recorder software) or by issuing a communication to the Data Subject confirming the verbal consent given (e.g. via the issuance of a letter, e-mail or SMS to the Data Subject).

1.10 In the context of principal and supplemental subscription accounts held by individual persons, the sufficiency of consent secured by the Data User would be dependent on the contract/documentation between the Data User and Data Subject. It shall be sufficient for purposes of compliance with the Act for Data Users to secure consent from the primary/principal Subscriber who executes the application or registration form encompassing both the principal and supplemental subscription accounts. However, where Data Users require the supplementary subscription account holder to execute a separate application or registration form, the consent of the primary/principal Subscriber will be insufficient to meet the consent requirement of the Act.

1.11 In the context of the relationship between Data Users and their corporate / business clientele that are legal entities, it shall be sufficient for purposes of compliance with the Act for Data Users to secure consent from the authorised representative of the legal entity for and on behalf of all individual subscribers from the said legal entity,

regardless of whether the authorised representative is an individual subscriber or not.

1.12 For the avoidance of doubt, any consent given to Data User by the authorised representatives of the Data Subject, including but not limited to the holders of any power of attorney, trustees, guardians or personal representatives, shall bind the respective Data Subject.

Processing Personal Data

1.13 Other than the issue of consent, the Act also sets out parameters for the processing of personal data, wherein personal data shall not be processed unless:

(i) the personal data is processed for a lawful purpose directly related to an activity of the Data User;
(ii) the processing of personal data is necessary for or directly related to that purpose; and
(iii) the personal data is adequate but not excessive in relation to that that purpose.

1.14 The criteria set out above are to be read conjunctively.

1.15 In the context of 1.13 of Part 3, directly above and this Code:

(i) *"directly related to that purpose"* means a purpose closely associated to the primary purpose;
(ii) *"necessary for … that purpose"* means without which the Data User would be unable to achieve the purpose; and
(iii) *"adequate but not excessive"* means just enough to enable the Data User to achieve the purpose, and no more.

1.16 To comply with the Act, a Data User is required to ensure that the personal data sought and held is:

(i) relevant in relation to the purpose(s) for which it has been collected;
(ii) adequate in relation to the purpose(s) for which it has been collected; and
(iii) not excessive in relation to the purpose(s) for which it has been collected.

1.17 The purpose or purposes for which a Data User collects and holds personal data of a Data Subject is required to be reflected in the Data User's Privacy Notice.

2.0 NOTICE AND CHOICE PRINCIPLE

2.1 Data Users are required to bring to the attention of Data Subjects their Privacy Notice, prior to or as soon as reasonably practicable, when collecting and processing their personal data.

2.2 In essence, the Privacy Notice is a publicly available statement clearly expressing the privacy practices of how a Data User uses, manages, discloses and provides Data Subjects with access to personal data collected by the said Data User. It is a general non-exhaustive statement about the privacy practices of the Data User that should result in Data Subjects having greater confidence in how the Data User will deal with their personal data.

Content Of The Privacy Notice

2.3 The Notice and Choice Principle specifically requires Data Users to provide Data Subjects with a notice stating:

(i) that personal data of the Data Subject is being processed by the Data User and providing the Data Subject with a description of the personal data being processed by the Data User;
(ii) the purpose(s) for which the personal data is being collected and processed;
(iii) the source of the personal data;
(iv) the Data Subject's right to access and correct the personal data and the contact details to which a Data Subject may send the Data Access and/or Correction Request;
(v) the class of third parties the personal data is disclosed or may be disclosed to;
(vi) the choices and means available to the Data Subject to limit the processing of his/her personal data;
(vii) whether it is obligatory or voluntary for the Data Subject to provide the personal data; and
(viii) where it is obligatory personal data, the consequences of failing to provide such obligatory personal data.

2.4 Where the Data User is an entity within a group of companies or a related corporation, it is permissible for the Privacy Notice to be issued by the group of companies instead, particularly in instances where there is shared infrastructure, back-end systems and operations. However, should an entity within a group of companies or a related corporation have its own Privacy Notice, the entity's Privacy Notice will override the Privacy Notice of the group of companies.

2.5 In cases where the Privacy Notice indicates that the personal data collected is to be disclosed to merchants and strategic partners, Data Users are required to provide Data Subjects with an option to opt-out of such disclosures. For the avoidance of doubt, this does not in any way preclude Data Users from providing an opt-in choice to Data Subjects.

2.6 The Privacy Notice needs to be provided in Bahasa Malaysia and English. Data Users may specify which version of the Privacy Notice will override the other in the event of a conflict in interpretation.

Communicating The Privacy Notice

2.7 The Privacy Notice is to be communicated by the Data User to the Data Subject either when the personal data is first collected, when the Data User first requests the Data Subject for the personal data, or as soon as practicable thereafter.

2.8 Data Users may communicate the Privacy Notice to Data Subjects by one or more of the following methods:

(i) by posting the Privacy Notice on the website of the Data User; or
(ii) by sending a message to Data Subjects with a website address / link to the Privacy Notice and/or a telephone number in order to request for the Privacy Notice and/or further information; or
(iii) by issuing an e-mail to Data Subjects with a website address / link to the Data User's Privacy Notice and/or telephone number to contact for further information; or
(iv) by inserting a summary notice in regular communications with Data Subjects (e.g. in monthly billing statements) with a website address / link to the Privacy Notice and/or a telephone number to contact for in order to request for the Privacy Notice and/or further information; or
(v) by inserting the Privacy Notice in application/registration forms; or
(vi) by inserting a statement in application/registration forms referencing the Privacy Notice, which may be accessed at a given website address, or by making a request to personnel of the Data User, or by calling a telephone number provided in the application/registration form; or
(vii) by printing out copies of the Privacy Notice and providing it to Data Subjects at the Data User's premises; or
(viii) any other recordable methods or means of delivery to Data Subjects as may be available or be adopted by Data Users.

2.9 Data Users are required by the Regulations to maintain records of having communicated the Privacy Notice to Data Subjects. The maintenance of the evidence of a process of communicating the Data Users Privacy Notice to its Data Subjects shall be sufficient to fulfil this requirement.

2.10 For the avoidance of doubt, each time the Data Subject utilises the Data User's services/facilities and is provided the Data User's Privacy Notice by way of any of the modes identified in 2.8 above, the Privacy Notice shall be deemed to have been communicated afresh to the Data Subject.

2.11 Proof of the Privacy Notice having been delivered, received and/or accepted by the Data Subject is not required under the Act.

3.0 DISCLOSURE PRINCIPLE

3.1 Data Users will only disclose the Data Subject's personal data pursuant to the terms of its Privacy Notice, the relevant provisions under the Act and/or such other applicable laws that the respective Data User is subject to.

3.2 A Data User can be taken to have *"disclosed"* personal data when it releases, communicates or disseminates the personal data of the Data Subject to third parties, whether intentionally or otherwise. The communication of the personal data may be in written or verbal form.

Permitted Disclosures

3.3 The Disclosure Principle provides that Data Users may disclose personal data to third parties where:

(i) the disclosure is for the purpose declared at the point of the collection of the personal data as stated in the Data User's Privacy Notice; or

Examples:

- *A Data Subject provides his/her information for the purpose of subscribing to telecommunication services. As a part of the process of activating the telecommunication service, the Subscriber's personal data needs to be provided to a third party to whom the Data User has outsourced a part of its operations (subject to technical and organizational security measures being in place in order to ensure the security of the personal data).*

(ii) the disclosure is for a purpose directly related to the purpose declared in the Privacy Notice at the point of the collection of the personal data (i.e. a purpose closely associated to the primary purpose); or

Examples:

- *A Data Subject defaults on his/her bills. The Data User disclose the relevant particulars of the Data Subject and his/her debt to a solicitor / debt collection agent to recover the amounts outstanding.*

(iii) the disclosure is being made to a third party mentioned in the Privacy Notice or to a class or category of third parties as identified in the Privacy Notice;

Examples:

- *Organizations that assist in fulfilling the transactions requested by the Data Subject.*
- *Parties authorised by the Data Subject (e.g. auditors, financial advisers).*

- *Merchants and strategic partners of Data Users.*
- *Credit reference agencies*

3.4 Other than the disclosures permitted based on the Privacy Notice as detailed in 3.3 above, the Act provides that Data Users may disclose personal data of Data Subjects should the following circumstances arise:

(i) the disclosure has been consented to by the Data Subject; or
(ii) the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or
(iii) the disclosure is required or authorized by or under any law or by the order of a court; or
(iv) the Data User acted in the reasonable belief that it had in law the right to disclose the personal data to the other person; or
(v) the Data User acted in the reasonable belief that it would have had the consent of the Data Subject if the Data Subject had known of the disclosure of the personal data and the circumstances of such disclosure; or
(vi) the Minister determines the disclosure as being justified in the public interest.

3.5 For the sake of completeness, Data Users are to note that the processing of personal data in certain instances have been excluded from compliance with the Disclosure Principle. These instances are briefly highlighted here:

(i) where personal data is processed for the prevention or detection of crime or for the purpose of investigations; or
(ii) where personal data is processed for the apprehension or prosecution of offenders; or
(iii) where personal data is processed for the assessment or collection of any tax or duty or any other imposition of a similar nature; or
(iv) where personal data is processed for the preparation of statistics or carrying out research (subject to the personal data not being processed for any other purpose and the resulting statistics or the results of the research being anonymised); or
(v) where personal data is processed for the purpose of or in connection with any order or judgment of a court; or
(vi) where personal data is processed for the purpose of discharging regulatory functions; or
(vii) where personal data is processed for journalistic, literary or artistic purposes.

Requests For Personal Data

3.6 In instances where Data Users receive requests from third parties for the disclosure of personal data, Data Users shall only disclose the requested personal data in the circumstances identified in 3.3 to 3.5.

3.7 In instances where requests for disclosure of personal data are directed to Data Users pursuant to a request of the police or any other investigating authority, or where the disclosure is required or authorized by or under any law or by an order of court, Data Users are required to:

(i) only release the requested personal data on a formal written request being made, citing the relevant legal basis of the request being so made; and
(ii) wherever appropriate, set conditions stipulating the permitted use of the personal data and its return or destruction upon the conclusion of the purpose of the requestor.

4.0 SECURITY PRINCIPLE

4.1 The Act does not prescribe the specific measures that need to be taken to secure the personal data within the control of Data Users, but instead requires Data Users to take *"practical steps"* to protect personal data from "*any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction"*.

4.2 What these *"practical steps"* amount to in real terms will vary from case to case, depending on the nature of personal data being processed by the Data User in question and the degree of sensitivity attached to the personal data or harm that the Data Subject might suffer due to its loss, misuse, modification, unauthorized or accidental access or disclosure, alteration of destruction.

4.3 The Act however does prescribe the elements that Data Users need to take into consideration when determining what practical measures need to be taken when securing their Data Subject's personal data. The prescribed elements are:

(i) 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;
(ii) the place or location where the personal data is stored;
(iii) any security measures incorporated into any equipment in which the personal data is stored;
(iv) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
(v) the measures taken for ensuring the secure transfer of the personal data.

4.4 The elements prescribed above are intended to keep personal data secure and as such apply to all Data Users.

Technical and Organizational Security Measures

4.5 The following technical and organizational security measures may be considered by Data Users and implemented wherever Data Users are of the view that it is required

or appropriate, such as, data classification policy, access control policy, confidentiality guidelines, technical security measures, anti-virus and anti-malware software, back-ups and encryptions. Descriptions of these technical and organizational security measures are set out below:-

(i) Organizational Security Measures

(a) **Data classification policy** – Personal data being processed by each Data User should ideally be categorised based on the sensitivity of the personal data and the harm that could arise vis-à-vis the Data Subject should the personal data be mishandled. The policy should identify the specific categories of personal data, the security measures associated with each of the said categories of personal data, both in physical and electronic formats.

(b) **Access control policy** – Personal data should be accessed by personnel of the Data User based on a *"need to know"* basis. Putting an access control policy in place will assist in this regard as the policy will indicate the various levels of personnel that are permitted access, modification and/or deletion rights in relation to different categories of personal data. It is recommended that access control policies should be supplemented with policies limiting access to technologies that allow personal data to be transferred out of the Data User's organization (as detailed further under technical security measures), and the activation of audit logs which enable authorised and unauthorised access to personal data to be traced.

(c) **Confidentiality guidelines** – It is recommended that guidelines in respect of the confidentiality of Data Subject information be issued (either separately or as part of the employee handbook) to all personnel of Data Users in order to make clear the fundamental importance of confidentiality and the role that it plays in establishing confidence and market credibility in the branding of the Data User. Further to this, it is recommended that employment contracts of Data Users explicitly state the obligation of maintaining the confidentiality of Data Subject information, and where there has been a breach of the same, Data Users need to be seen to have taken the necessary action in order that personnel are aware of how seriously Data Users take this issue.

(ii) Technical Security Measures

(a) **Physical document security** – Physical documents such as service application forms, copies of identity documents, letters, need to be received, processed and stored securely.

(b) **Physical access to IT facilities** – Access to IT facilities where the IT infrastructure (such as servers, networks, routers) and the

telecommunications infrastructure (exchanges and junction boxes) of Data Users are located, needs to be controlled at all times. This can be achieved through the use of security guards for perimeter and location security, escorts in order to allow guests into the IT facility, tags to identify authorised personnel, card / biometric based access systems to regulate access, and the use of CCTV monitoring for overall monitoring.

(c) **Physical access to IT systems and communications equipment** – Access to IT systems within Data Users offices or premises such as PCs, tablets, printers and fax machines needs to controlled at all times as personal data may be stored and/or displayed on them. This can be achieved through restricting physical access to any non-authorised personnel, careful positioning of PCs in order to ensure that screens are not viewable by non-authorised personnel, the utilisation of screen savers for unattended PCs, and locked printer and/or fax rooms which are accessible only to authorised personnel.

(d) **Back-ups** –Data Users should back-up the personal data resident on their systems in order to guard against data loss. The media on which the back-ups are resident should be stored off-site to prevent their loss together with the primary systems in the event of a major disaster.

(e) **Anti-virus and anti-malware software** - Data Users would be required to install and regularly update their anti-virus software in order to avoid putting the personal data of Data Subjects at risk via virus infections and other malware. Personnel should be restricted from downloading and installing applications that have not been approved by the IT department of the Data User as it may introduce malware which may put personal data at risk.

(f) **Securing access** - All personal data that is removed from the premises of the Data User with authorisation, whether on notebooks, tablets, smart phones, USB thumb drives, portable hard drives, are to be secured in order to prevent the personal data stored on the said devices being accessed without authorisation in the event the said devices being stolen or lost. E-mails attaching personal data are also to be secured in order to prevent the personal data being accessed by unauthorised third parties.

4.6 Upon due consideration, Data Users may choose not to put any of the organizational or technical security measures mentioned above in place. In such cases, Data Users are required to put into place alternative mechanisms that address the risk of loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction of personal data.

Data Processors

4.7 The Security Principle also addresses the processing of personal data by data processors for and on behalf of Data Users.

4.8 Typically, data processors are third parties such as outsourcing service providers or any vendors (including but not limited to security, transportation, accounting, postal service providers) that are appointed to process the personal data of Data Subjects for and on behalf of the Data User alone. In this context, the word *"process"* should be interpreted as per the definition in the Act.

4.9 The Security Principle permits the processing of personal data by data processors, but requires the Data User to take certain minimum measures in order to ensure that the personal data of Data Subject is not subject to the risk of loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. These measures include:

(i) the data processor giving the Data User *"sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out"*; and
(ii) the Data User taking *"reasonable steps to ensure compliance with those measures"*.

4.10 Data Users are required to utilise reasonable efforts to raise and negotiate the technical and organizational security measures required by the Data User from the data processor for the purposes of fulfilling the Security Principle. Data Users should determine in each case which of the technical and organizational security measures apply to the data processor.

4.11 It is recommended that Data Users use their reasonable efforts to ensure that their agreement with data processors (whether in the form of a contract or letter or otherwise) addresses the following matters:

(i) the data processor's undertaking to ensure that neither itself nor its employees disclose the personal data to any third party without the authorisation of the Data User;
(ii) the data processor's undertaking to deploy the agreed technical and organizational security measures, as well as the obligation to inform the Data User should any of the measures be breached;
(iii) the data processor's undertaking to otherwise conduct itself in such a manner so as to not cause the Data User to breach the Act;
(iv) the obligation of the data processor to return all the personal data upon expiry or termination of the agreement term; and
(v) the right of the Data User to conduct an audit (on-site or via questionnaire) of the technical and organizational security measures should it so require.

4.12 Data Users should note that data processors may be based either locally or abroad, and should adjust their agreements or binding letters or any other relevant documentation appropriately.

Commissioner's Security Standards

4.13 Data Users are required to also comply with any security standards as may be set out by the Commissioner from time to time.

4.14 For the avoidance of doubt, in the event of a conflict between the Commissioner's security standard, this Code, any security standard(s) (or their equivalent) set by the Communications and Multimedia Commission of Malaysia or such other regulators of the Data User and/or any security standard(s) (or their equivalent) prescribed by the law, the document setting the higher standard will prevail to the extent of the conflict.

5.0 RETENTION PRINCIPLE

5.1 The Act places a responsibility on Data Users to hold personal data only for as long as necessary for the fulfilment of the purpose. The Act also provides that upon the purpose being fulfilled, Data Users are required to permanently destroy/delete the personal data. This requirement applies to both physical and electronic copies of documents containing personal data.

5.2 For the avoidance of doubt, the Act does not override other applicable statutory provisions that require the retention of data/records/information for a specified minimum duration, for instance, the Companies Act 1965, Income Tax Act 1967, Employment Act 1955 or the Limitation Act 1953. The Act and such other applicable legislation must be read together.

Applicable Retention Periods

5.3 This Code does not specify the applicable durations that personal data may be retained for but leaves it to the discretion of Data Users.

5.4 In order to assist Data Users to keep track of the various retention periods as may be applicable to the various types of personal data processed by them, Data Users are required to consolidate all applicable retention periods into the Data User's relevant retention policies which addresses the various categories of personal data, for example:

(i) Application forms
(ii) Unsuccessful applications
(iii) Call records
(iv) Customer audio recordings

(v) Defaulting customers

5.5 There may be certain instances in which Data Users need to retain personal data beyond a specified statutory period. In these cases, Data Users should be able to demonstrate a reasonable need to retain personal data beyond the applicable statutory period and (if available) provide evidence of their adherence to the same. The commencement of legal proceedings or investigations concerning the Data Subject would qualify as grounds for continuing to retain the personal data until the disposal/closure of the matter and the expiry of the retention period specific to the matter itself.

5.6 For the avoidance of doubt, the Retention Principle does not apply to backup and electronic archival data subject to the Data User restricting access to the same to authorised personnel only and for backup or archival purposes respectively.

Destruction / Permanent Deletion of Personal Data

5.7 The Act requires the *"destruction"* (applicable to physical / paper based personal data) and *"permanent deletion"* (applicable to electronic personal data) of personal data once the conditions of disposal are met.

5.8 For the avoidance of doubt, Data Users are to note that personal data that is physically archived are still subject to the provisions of the Act and will continue to remain so until it is destroyed, permanently or anonymized. Bearing in mind the volume of records containing personal data that are required to be destroyed / permanently deleted or anonymized, Data Users shall be permitted a period of five (5) years from the effective date of this Code to ensure that the necessary measures are adopted in respect of their physical archives.

5.9 As an alternative to destroying or permanently deleting the personal data, Data User can also consider the process of anonymizing the personal data instead. Where properly anonymized, the anonymized data will not fall within the ambit of the definition of *"personal data"* as it will no longer contain any linkage to the individual in question.

Commissioner's Retention Standards

5.10 Data Users are required to comply with any retention standards as may be set out by the Commissioner from time to time.

5.11 For the avoidance of doubt, in the event of a conflict between the Commissioner's retention standard, this Code, any retention standard(s) (or their equivalent) set by the Communications and Multimedia Commission of Malaysia or such other regulators of the Data User and/or any retention standard(s) (or their equivalent) prescribed by the law, the document setting the higher standard will prevail to the extent of the conflict.

6.0 DATA INTEGRITY PRINCIPLE

6.1 The Act provides that a Data User is to take *"reasonable steps"* to ensure that the personal data processed by the Data User is *"accurate, complete, not misleading and kept up-to-date"*, in relation to the purpose.

6.2 By way of illustration, the Act requires a Data User to take reasonable steps in order to ensure that the personal data processed in relation to a Data Subject is:

(i) accurate / correct (meaning that the personal data is captured without any inaccuracies, such as erroneously recording the Data Subject's agreement to receive direct marketing materials for other products of the Data User);
(ii) complete (meaning that information in relation to the Data Subject has not been omitted, which for example may lead the Data User to make an unfavourable decision in relation to a Data Subject's application for services);
(iii) not misleading (meaning that the personal data processed by the Data User should not - through error, omission, oversight, etc. - result in an inaccurate or false reflection of the status of the Data Subject); and
(iv) kept up-to-date (meaning the personal data of the Data Subject should reflect the latest information as provided by the Data Subject).

6.3 What amounts to *"reasonable steps"* will 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 and the frequency of communications with the Data Subject.

6.4 Notwithstanding the foregoing, Data Users are entitled to treat the personal data provided by Data Subjects as accurate, complete, not misleading and up-to-date. Data Users are not required to verify the accuracy and completeness of the personal data provided by Data Subjects, except in the case of clear and obvious inaccuracies.

6.5 The Act shall not override any agreement between the Data User and Data Subject which specifies that it shall be the duty of the Data Subject to inform the Data User of any change to the Data Subject's information (such as a new address or telephone number), and the Data User shall not be found to be in breach of the Data Integrity Principle where the Data User has not been so informed by the Data Subject.

6.6 Similarly, where the Data User provides a self-update facility to the Data Subject which permits the Data Subject to update his/her personal data, the Data User shall not be found to have breached the Data Integrity Principle should the Data User act based on the wrong personal data provided by the Data Subject.

6.7 For the avoidance of doubt, the following are not breaches of the Data Integrity Principle:

(i) maintenance of personal data which is historical in nature (for example, the previous address that the Data Subject used to reside at when he/she commenced subscribing to the communications service by the Data User), subject to the same being accurate; and

(ii) maintenance of personal data that records events that happened in error, subject to those records not being misleading about the facts (for instance where a Data Subject's subscription was wrongfully terminated but has since been reinstated, the Data User would be permitted to retain the said records as it accurately reflect the error on the part of the Data User).

Commissioner's Data Integrity Standards

6.8 Data Users are required to comply with any data integrity standards as may be set out by the Commissioner from time to time.

6.9 For the avoidance of doubt, in the event of a conflict between the Commissioner's data integrity standard, this Code, any data integrity standard(s) (or their equivalent) set by the Communications and Multimedia Commission of Malaysia or such other regulators of the Data User and/or any data integrity standard(s) (or their equivalent) prescribed by the law, the document setting the higher standard will prevail to the extent of the conflict.

7.0 ACCESS PRINCIPLE

7.1 The Act provides Data Subjects with the right:

(i) to request access to his/her personal data held by Data Users; and/or

(ii) to correct his/her personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date,

unless the request is one which Data Users may deny as stated in the Act.

7.2 Data Users are obliged to respond accordingly to these data access and data correction requests within fixed timelines as detailed in Part 5, in order to remain compliant with the Act.

7.3 Data Users have the right not to comply with a data access request where Data Users:

(i) have not been supplied with sufficient information (as reasonably required, i.e. name, identification card number, address, and such other related information as the Commissioner may determine) in order to establish the requestor's identity, establish the identity of the Data Subject, or establish the requestor's connection to the Data Subject; or

(ii) have not been supplied with sufficient information as they may reasonably require to locate the personal data to which the data access request relates; or

(iii) are unable to comply with the data access request without disclosing another person's personal data (unless the other person has consented to the disclosure of the personal data to the requestor); or

(iv) are of the view that the burden or expense of providing access is disproportionate to the risks to the Data Subject's privacy in relation to the personal data requested for via the data access request; or

(v) are at risk of violating a court order should they provide access to the Data Subject or requestor; or

(vi) are of the view that that providing access would disclose confidential commercial information of the Data User; or

(vii) are of the view that that providing access would disclose confidential commercial information of the Data User.

7.4 Other than the above, Data Users are to note that the processing of personal data in certain instance have been excluded from compliance with the Access Principle. These instances are briefly highlighted here:

(i) where personal data is processed for the prevention or detection of crime or for the purpose of investigations; or

(ii) where personal data is processed for the apprehension or prosecution of offenders; or

(iii) where personal data is processed for the assessment or collection of any tax or duty or any other imposition of a similar nature; or

(iv) where personal data is processed for the preparation of statistics or carrying out research (subject to the personal data not being processed for any other purpose and the resulting statistics or the results of the research being anonymised); or

(v) where personal data is processed for the purpose of or in connection with any order or judgment of a court; or

(vi) where personal data is processed for the purpose of discharging regulatory functions; or

(vii) where personal data is processed for journalistic, literary or artistic purposes.

7.5 Please refer to Part 5 where the Data Subject's rights of access and correction are further addressed.

PART 4
SPECIFIC ISSUES RELEVANT TO THE MEMBERS OF THE CMA DATA USER FORUM

1.0 PERSONAL DATA

1.1 Data Users processes a substantial amount of data in its day to day operations, some of which can be considered to be personal data, while others are not as considered personal data due to the data not meeting one or more requirements of the Act.

1.2 For the purpose of clarity, the following types of data fall outside the ambit of the Act and are therefore not considered to be *"personal data"*:

(i) Data relating to organizations
(ii) Data relating to deceased individuals
(iii) Data pertaining to individuals that have been aggregated and/or anonymised in such a manner as to render the individual non-identifiable
(iv) Data that is electronically archived and/or backed up

1.3 In so far as organizations / companies, the information of their officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, suppliers/vendors and/or related parties are provided by the said organizations/companies to Data Users for the purpose of securing subscription accounts or such other facilities from the said Data Users, the said information shall be treated as information that the said organization / company is authorised to provide to the Data User.

1.4 For the avoidance of doubt, Data Users are not required to obtain consent from the said officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, suppliers/vendors and/or related parties, in order to process said information for the purpose of the organization / company securing subscription accounts or such other facilities or products from the said Data Users.

1.5 However, in instances where the Data User utilises the data of the officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, suppliers/vendors and/or related parties of the company / organization for a commercial purpose not related to the company / organization (for example, offering an employee of a company one or more telecommunication / broadcast subscription services in his personal capacity), the said officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, suppliers/vendors and/or related parties shall be considered to be Data Subjects and shall be entitled to rights under the Act.

2.0 SENSITIVE PERSONAL DATA

2.1 The Act defines Sensitive Personal Data as *"any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette"*.

2.2 An example of sensitive personal data that may be collected in the course of providing communication services to Data Subjects includes the collection or the scanning of copies of a customer's identification card which indicates the religion of the said customer (either expressly for Muslims or by implication for non-Muslims).

2.3 Section 40 of the Act provides that a Data User shall not process the Sensitive Personal Data of a Data Subject, unless the Data Subject has given his/her *"explicit consent"* or where, for example, the processing is necessary for :

(i) the purpose of any legal proceedings; or
(ii) the purpose of obtaining legal advice; or
(iii) establishing, exercising or defending the Data User's legal rights.

2.4 In the context of Data Users, the collection of NRIC information is central to the opening of accounts for customers of Data Users and for the on-going management of their subscriptions. Frequently, this takes the form of photocopying or scanning the entire NRIC and returning the original to the customers, while the copy is retained in physical or electronic format by the Data User. Where this is done, the Data User concerned may be in possession of information pertaining to the Data Subject (i.e. whether the customer is a Muslim or a non-Muslim). In these instances, the *"explicit consent"* of the customer would be required under the Act.

Processing Of Sensitive Personal Data Where The Data Subject Provides Explicit Consent

2.5 The Act does not define what is meant by *"explicit consent"*.

2.6 However, the Regulations provide that any *"consent"* obtained needs to be capable of being *"recorded"* and *"maintained"*. As such, it may be presumed that the same requirements that apply to consent for processing personal data, apply to Sensitive Personal Data as well.

Form Of Explicit Consent

2.7 Verbal explicit consent would arise in instances where a Data Subject provides a verbal statement giving consent for the processing of his/her Sensitive Personal Data. Bearing in mind the stipulations of the Regulations in relation to consent (i.e. that consent needs to be capable of being *"recorded"* and *"maintained"*), it is

recommended that any verbal consent given by the Data Subject should be recorded, for example via an audio recording or via a confirmatory e-mail, in order to fulfil the requirements specified within the Regulations.

2.8 Explicit consent can also be obtained via the conduct of a Data Subject. Examples of conduct amounting to explicit consent include where the Data Subject:

(i) proceeds to volunteer his/her sensitive personal data (e.g. the provision of the information on the Data Subject's NRIC); or
(ii) continues to utilise the services of the Data User,

subject to compliance with 2.0 of Part 3 of this Code.

2.9 All other forms of explicit consent given by the Data Subject would need to be in writing (as per the definition in Part 2) and indicate the Data Subject's agreement to the processing of his/her Sensitive Personal Data by the Data User. Acceptable forms of written explicit consent include:

(i) any form of writing indicating the Data Subject's explicit consent as to the processing of his/her personal data; or
(ii) a signature or tick of the Data Subject indicating his/her explicit consent.

3.0 PRE-EXISTING DATA

3.1 This Code shall apply to all data that is in the possession or under the control of Data Users as of 15th November 2013 and that meet the necessary criteria in order to be recognised as *"personal data"*. For the avoidance of doubt, this would include personal data collected and or otherwise processed by the Data User prior to 15th November 2013.

3.2 Notwithstanding the foregoing paragraph, where:

(i) the personal data relates to inactive, closed or dormant accounts, Data Users shall utilise their commercially reasonable efforts to comply with the Act and this Code; and
(ii) where data is held in electronic archives and/or in electronic/tape backup media, the said data shall not be subject to the Act for so long as the Data User restricts access to the data to authorised personnel only and for backup or archival purposes respectively.

3.3 In instances where the personal data relate to accounts that are active or to data that has been reinstated from the backups or the electronic archives of the Data User, Data Users are required to fully comply with the Act and Code.

4.0 DIRECT MARKETING

4.1 The Act permits Data Users to conduct direct marketing of products and services to Data Subjects, subject to the caveats laid out herein.

4.2 Section 43(5) of the Act defines *"direct marketing"* as *"the communication by whatever means of any advertising or marketing material which is directed to particular individuals"*.

4.3 The Act does not define what is meant by *"communication"*, *"advertising or marketing material"* or *"directed to particular individuals"*. However, in most cases:

(i) *"communication"* includes the unsolicited communication via personal interaction, door-to-door sale calls, post, telephone, fax, e-mail, SMS, other internet / social / application based messaging systems;
(ii) *"advertising or marketing material"* refers to the promotional material of the Data User or of parties other than the Data User; and
(iii) *"directed to particular individuals"* means that the individual needs to be identified or be selected based on the use of his/her personal data.

4.4 Based on the above, the communication by Data Users of advertising or marketing material (via mediums such as mail or SMS) to particular individuals selected based on the use of their personal data, qualifies as direct marketing for the purposes of the Act as the communication is *"directed"* at those particular individuals.

4.5 However, marketing materials that are not directed at particular individuals but are instead sent to **all** customers of a Data User or to an entire category/type of customers (e.g. all broadband customers of a Data User) of a Data User, will not be considered direct marketing for the purposes of the Act and Code as it is not being directed at particular individuals.

4.6 It is critical to note that not all marketing falls under the scope of the Act. Where advertising or marketing material is communicated without knowledge of who the actual recipients are, for example where mails are sent to *"the occupant"* of residences within a neighbourhood and the sender has no knowledge as to the identity of the respective individuals, the Act will clearly not be applicable. Similarly, SMSes that are sent by the sender without knowledge of who the actual recipient is or non-targeted advertising conducted via the Data User's website, clearly do not fall within the ambit of the Act.

Notice And Consent

4.7 Data Users communicating advertising or marketing material directed to particular individuals, through the utilisation of the said Data Subject's personal data (e.g. name, address, mobile phone numbers, e-mail address) which was provided by:-

(i) the Data Subject in the course of signing up for products or services of the Data User; or

(ii) Data Subjects who are not customers of the Data User but who have expressed an interest in the products or services of the Data User (for example, where the Data Subject calls up the customer service department of a Data User making enquiries in respect of its products and services),

should either have already notified the Data Subjects of the same via their respective Privacy Notices (as detailed in 4.8 below), or in cases where their Privacy Notices are silent as to the issuance of such advertising or marketing material, should obtain the consent of the Data Subject prior to commencing direct marketing.

4.8 Specifically, Data Users conducting direct marketing are required to notify their Data Subjects:-

(i) that their personal data will be used for the purposes of direct marketing;

(ii) of the class of third parties the personal data is disclosed or may be disclosed to (e.g. to the Data User's strategic business associates, preferred merchants); and

(iii) of the right of Data Subjects to refuse such use (for direct marketing / cross selling purposes) of their personal data at any time by way of providing a notice in writing to the Data User.

4.9 Data Users may provide such notifications to Data Subjects via their Privacy Notice which are to be disseminated to Data Subjects in compliance with the requirements of the Notice and Choice Principle. Please refer to 2.0 of Part 3 for further details on the content of the Privacy Notice.

Obtaining Personal Data From Other Sources

4.10 Data Users are permitted to obtain personal data of individuals (that are not their customers or that they do not have a pre-existing relationship with) for the purpose of directing marketing from third party sources subject to Data Users taking practical steps to ensure that the said third party sources or by referral from Data Subjects themselves.

4.11 However, Data Users are required to take practical steps to ensure that the necessary notices and/or the relevant consents of the said individual for the disclosure of their personal data to the Data User for the purposes of direct marketing have been obtained.

4.12 Data Users may do so by entering into written agreements with such third parties, wherein adequate representations and warranties are provided by the third parties, i.e. that the relevant consent to disclose personal data has been obtained from the Data Subject prior to its disclosure to the Data User.

4.13 Using or processing personal data sourced from publicly available sources of information (such as the Companies Registry at the Suruhanjaya Syarikat Malaysia, the National Land Registry, personal Facebook pages or the World Wide Web) for the purpose of direct marketing to individuals is prohibited, as the Data Subject has:

(i) provided the said personal data for purposes other than direct marketing; and
(ii) not been notified of or consented to receiving direct marketing.

4.14 Notwithstanding the foregoing, Data Users are not barred from contacting Data Subjects for the purpose of establishing the Data Subject's interest in the services provided by the Data User, subject at all times to the maintenance of a system or process to maintain the details of those Data Subjects that choose to opt-out of receiving any future marketing communications from the Data User.

Appointment Of Marketing Agents

4.15 Where a Data User engages a third party (i.e. a data processor) to conduct direct marketing on its behalf, for example a mailing house to mail out its direct marketing materials, Data Users are to impose certain requirements upon the marketing agent as laid out in 4.16.

4.16 For all new contracts entered into between the Data User and the marketing agent, the Data User shall on a reasonable efforts basis ensure that any processing of personal data by the marketing agent takes place subject to a contract between the Data User and the marketing agent which specifies:

(i) the conditions under which the personal data may be processed;
(ii) the representations, undertakings, warranties and/or indemnities which are to be provided by the marketing agent;
(iii) the technical and organizational security measures governing the processing to be carried out as may be contained in a Data User's internal security policy and/or standards;
(iv) steps to ensure compliance with those measures, for instance submitting to on-site audits, completing personal data compliance questionnaires or obtaining declarations of compliance; and
(v) the deletion, destruction and/or the return of the personal data that is under the control of the marketing agent upon completion or termination of the contract.

4.17 In recognition of the fact that existing agreements of the Data User with marketing agents may not cater for the above, this Code requires Data Users to utilise their reasonable efforts to modify said agreements accordingly but failure to do so shall not result in a breach of the Act.

Data Subject's Right To Refuse Direct Marketing

4.18 As stated in 4.8(iii), Data Users are to provide all Data Subjects with the right to refuse the use of their personal data for direct marketing purposes.

4.19 Such requests can be made:-

(i) via the initial application form when signing up for products/services through an opt-out tick-box; or
(ii) in direct marketing communications with the Data Subject, the Data User includes a prominent statement, or otherwise draws the Data Subject's attention to the fact that the individual may make such a request; or
(iii) in relation to e-mail marketing, the Data Subject can opt out of receiving future direct marketing emails by replying with a single word instruction in the subject column (for example, 'unsubscribe'); or
(iv) in relation to text message marketing, the Data Subject can opt out of future direct marketing by utilising the measures prescribed by the Data User; or
(v) in relation to phone call marketing, clearly telling Data Subjects that they can verbally opt out from any future direct marketing calls; or
(vi) via a letter from the Data Subject to the Data User; or
(vii) via any other identified mode of communication,

and needs to be provided to the Data Subject without charge.

4.20 It is recommended that a systematic approach be adopted by the Data User to effectively comply with a Data Subject's request to cease direct marketing.

Right To Prevent Processing Of Personal Data For Purposes Of Direct Marketing

4.21 A 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/her personal data for purposes of direct marketing. A Data User is required to comply with the written notice at the end of such period as is reasonable in the circumstances.

4.22 This is further addressed in Part 5 of this Code.

5.0 CREDIT REPORTING AGENCIES

5.1 Information regarding Data Subjects obtained from credit reporting agencies ("CRA") is considered to be personal data falling under the ambit of the Act.

Access To Consumer Credit Data

5.2 Data Users may access the credit data of a Data Subject held by the CRA (e.g. through a credit report provided by the CRA), for example in the process of:-

(i) considering the grant of an application for the Data Users products/services by conducting appropriate checks for credit-worthiness and for fraud checking; or
(ii) a review of an existing product/service granted to the Data Subject (e.g. where there is a request for an increase in credit amount); or
(iii) the renewal of an existing product/service granted to the Data Subject,

subject to notification being provided to Data Subjects on the collection of consumer credit data and the purpose for doing so (e.g. conducting checks for credit-worthiness) via their respective Privacy Notices and/or obtaining the consent of Data Subjects.

Disclosure of Credit Data

5.3 Data Users are permitted to disclose the personal data of Data Subjects to CRAs:-

(i) upon an application for a product and/or service;
(ii) upon the Data Subject defaulting in payment; and/or
(iii) upon the termination of the Data Subject's account.

5.4 Data Users may obtain the consent of Data Subjects for the collection and processing of consumer credit data by inserting appropriate consent clauses within the terms and conditions governing the Data User's relevant services / facilities.

Defaulters Database

5.5 Data Users are permitted to maintain a listing of Data Subjects that have absconded without payment or have defaulted in respect of communication services rendered with one or more commonly appointed CRAs. The said CRAs will maintain such databases based on the relevant or updated personal data of Data Subjects as forwarded to the CRAs by Data Users.

5.6 Each Data User is permitted to conduct credit checks utilising the said databases prior to registering new customers or in managing the subscriptions/accounts of Data Subjects.

6.0 CERTIFICATE OF REGISTRATION

6.1 Data Users are required by the Regulations to display:

(i) the original Certificate of Registration issued by the Commissioner pursuant to the Act at the Data User's principal place of business (for example, the Data User's headquarters); and

(ii) copies of the Certificate of Registration that have been certified by the Commissioner at each of the branches of the Data User (for example, the Data User's customer service centres),

(hereinafter collectively referred to as "Certificates").

6.2 For the purpose of interpretation, a "branch" shall mean one or more branches operated by the Data User where interaction occurs with Data Subjects. For the avoidance of doubt, kiosks, exchanges, offices of the Data User where there is no interaction with Data Users, premises operated by marketing agents or dealers, and/or the premises of data processors, shall not be deemed to be branches for the purposes of this Code.

6.3 Data Users may display the Certificates on notice boards within the premises, on electronic displays, on the screens of self-service terminals and/or on the websites of Data Users. Where the Certificates are displayed at the relevant premises on electronic screens or their equivalent, Data Users are hereby exempted from displaying the actual certificate, but will be required to produce the same for the purposes of inspection by the Commissioner.

6.4 For the avoidance of doubt, there is no need for Certificates to be displayed at the premises or kiosks of marketing agents or resellers of the Data User.

6.5 Not displaying one or more Certificates shall not be an offence under the Act or its Regulations where the Certificates have been applied for but have yet to be issued by the Commissioner subject at all times to the provision of the proof of filing or the relevant receipt.

7.0 TRANSFER OF PERSONAL DATA ABROAD

7.1 The Act prohibits the transfer of personal data to a place outside of Malaysia unless the transfer is to a place with data protection laws substantially similar to the Act or which ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the Act, as specified by the Minister in a Government Gazette, based on the Commissioner's recommendation to the Minister.

7.2 Notwithstanding the above-mentioned prohibition, the Act expressly permits the transfer of personal data abroad where:

(i) the Data Subject has consented to the transfer; or
(ii) the transfer is necessary for the performance of a contract between the Data User and the Data Subject (for example the provision of international roaming services to a customer); or

(iii) the transfer is necessary to perform or conclude a contract between the Data User and third party which has been entered into at the request, or in the interest, of the Data Subject; or
(iv) the transfer is for legal proceedings or obtaining legal advice; or
(v) the Data User has reasonable grounds for doing so; or
(vi) the Data User has taken reasonable precautions to ensure the personal data will not be processed in any manner which contravenes the Act; or
(vii) the transfer is necessary to protect the vital interests of the Data Subject (this would relate to matters of life and death as defined in the Act); or
(viii) the transfer is necessary as being in public interest as determined by the Minister.

7.3 Based on the above, Data Users are to use all reasonable efforts to:

(i) address the issue of the transfer of personal data abroad either within their respective Privacy Notices or by addressing the same within the contract between the Data User and Data Subject; and
(ii) ensure that binding letters are exchanged or appropriate contractual clauses are inserted into contracts with overseas recipients of personal data, in order to safeguard the transferred personal data as required by the Act, as expanded in 7.4 below.

7.4 It is recommended that Data Users take reasonable steps to ensure that any overseas recipients of personal data (for example overseas mobile operators) are contractually bound:

(i) not to use the Data Subject's personal data for any reason other than to provide the relevant products or services, and
(ii) to adequately safeguard the Data Subject's personal data.

PART 5
RIGHTS OF DATA SUBJECTS

1.0 RIGHTS OF ACCESS TO PERSONAL DATA

1.1 Under the Access Principle, any individual, whether or not the individual is a customer of the Data User, 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 set in the Act.

1.2 Other than the individual himself/herself, the persons who may make a DAR on behalf of the said individual are:

(i) the parent, guardian or person who has parental responsibility for an individual below the age of 18; or
(ii) a person appointed by a court to manage the affairs of the individual; or
(iii) a person authorised in writing by the individual to act on the individual's behalf; or
(iv) a person authorised in writing by the individual to make a DAR on behalf of the individual.

1.3 For the purpose of Part 5, the term "Data Subject" shall be deemed to include individuals whose personal data has never been processed by the Data User.

Ambit Of A DAR

1.4 A DAR may be made in respect of personal data provided by the Data Subject to the Data User during registration and any updates thereto that are currently within the various electronic and physical systems of the Data User.

1.5 Data Users are required to ensure that the personal data that is sought by the Data Subject is provided to the Data Subject in an *"intelligible form"*. *"Intelligible form"* has not been defined in the Act, and as such should be interpreted utilising the normal dictionary meaning, wherein a Data Subject must be able to understand/comprehend the information supplied without having to revert to the Data User for an explanation. For example, where a Data User holds personal data in specific abbreviations, codes or other undefined terms, the same ought to be explained to the Data Subject in a manner a layperson is able to understand.

1.6 For the avoidance of doubt, personal data being retained for backup and archival purposes are not subject to the Access Principle.

Making A DAR

1.7 The Regulations provide that where a Data Subject does not require a copy of the personal data, the Data Subject must inform the Data User in writing of the Data

Subject's intention of making a DAR. This would presuppose that Data Users are required to provide Data Subjects with a choice at the point of making a DAR, of either:

(i) confirming whether or not the Data User retains any personal data in respect of the said Data Subject; or
(ii) providing the Data Subject with the personal data that the Data Subject is seeking as per 1.4 above.

1.8 A DAR needs to be specific as to the personal data that is being sought. In this context, a request for "all personal data" shall not be considered to be a proper DAR.

1.9 Where a Data Subject has separate accounts with a Data User, separate DARs may be required by the Data User for each account.

Format Of A DAR

1.10 A DAR does not have to be in a particular format. However, there are prerequisites that a Data Subject or a third party requestor ("requestor") must fulfil when making a DAR:-

(i) the DAR must be in writing in a form acceptable to the Data User;
(ii) the necessary payment needs to have been enclosed together with the DAR;
(iii) the necessary information and documentation as may be required by the Data User in order to locate the personal data being requested (e.g. name, NRIC / passport number, address, account number and personal data being sought);
(iv) the DAR must be specific as to the personal data that is being sought; and
(v) relevant certified documentation is to be submitted in order to establish the Data Subject or the requestor's right to make a request.

If any one of these prerequisites is not fulfilled, the Data User ought to return the DAR to the Data Subject / requestor and request that the omitted information / payment / copies be resubmitted by the Data Subject / requestor.

1.11 Data Users may require the use of a standardised form for a DAR to be made by a Data Subject / requestor. A standardised form will assist Data Users in determining the type of access request that the Data Subject / requestor is making, the specific personal data being sought and how the response is to be communicated to the Data Subject / requestor, amongst others. Additionally, it will assist the Data Subject / requestor by making clear what information and documentation is required to be submitted together with the DAR.

1.12 In instances where a Data User receives a verbal request for access to personal data, the Data User is not required to respond to the request. However, the Data User should guide the Data Subject / requestor on the proper manner of making a valid

DAR and provide whatever assistance as may be required by the Data Subject / requestor to make a DAR.

1.13 The maximum fees that a Data User may impose for a DAR are:

Description	Maximum Fees That Data Users May Impose (RM)
DAR for an individual's personal data without a copy	2
DAR for an individual's personal data with a copy	10
DAR for an individual's sensitive personal data without a copy	5
DAR for an individual's sensitive personal data with a copy	30

Receipt And Processing Of A DAR

1.14 In line with the Regulations, a Data User is to provide written acknowledgement of having received the DAR, upon:-

(i) confirmation of the identity of the Data Subject / requestor;
(ii) submission of relevant certified documentation to establish the requestor's right to make a request on behalf of the Data Subject;
(iii) the submission of the relevant processing fee(s); and
(iv) the personal data being sought being clearly specified.

1.15 In the event the Data Subject's NRIC details do not correspond with the Data Subject's details on record, or the documentation proving the requestor's right to act on behalf of a Data Subject being insufficient, or the fees not being submitted, or the personal data not being clearly specified, Data Users have the right to require the Data Subject or requestor to verify their identity to the Data Users' satisfaction.

1.16 Where the Data User is of the view that it is necessary and/or appropriate (e.g. where there is suspicion of deception / false or misleading information is provided / insufficient documentation provided), it may contact the said Data Subject at his/her last known telephone number / facsimile number / e-mail address in order to confirm that the DAR is legitimate.

1.17 Where the Data User is unclear as to the specific personal data that is being sought by the Data Subject / requestor, the Data User may request for further information, e.g. account numbers, dates of communication, or description of the interaction with the Data User.

1.18 Once the Data User has all the necessary information required in order to process the DAR, the personal data being sought is to be located and provided to the Data

Subject / requestor in question, except for instances in which such DARs may be rejected as provided for in the Act and further in 1.21 below.

1.19 Data Users are required by the Act to revert in writing to the person making the request within twenty-one (21) days from the date of receipt (i.e. date of acknowledged receipt) of the DAR. Where the initial twenty-one (21) days is insufficient, Data Users are required to dispatch a letter to the said Data Subject / requestor informing them of the delay and the required extension, subject to it not being in excess of fourteen (14) days.

1.20 In the event that only some of the personal data can be located, Data Users are obliged by the Act to provide the Data Subject / requestor with the sought after personal data to the extent that they are able to do so, whilst informing the said Data Subject / requestor of the efforts being undertaken to provide the balance of the personal data.

Refusal To Comply With A DAR

1.21 Where a Data User does not comply with a DAR based on the reasons provided section 32 of the Act, the Data User is to provide the Data Subject or the requestor of the DAR with written notification of the refusal to comply and supporting reasons.

1.22 Pursuant to section 32 of the Act, Data Users have the right not to comply with a DAR where:

(i) the Data User has not been supplied with sufficient information as reasonably required (e.g. the name, identification card number, address, and such other related information as the Commissioner may determine) in order to establish the identity of the Data Subject / requestor, or establish the requestor's connection to the Data Subject; or

(ii) the Data User has not been supplied with sufficient information as it may reasonably require to locate the personal data to which the DAR relates; or

(iii) the Data User is unable to comply with the DAR without disclosing a third party's personal data (unless the other person has consented to the disclosure of the personal data to the Data Subject/requestor). The Data User is required to in this situation balance the Data Subject's rights of access to personal data against the third party's privacy rights in relation to their personal data. In doing so, the Data User may consider the following steps:-

- anonymising the personal data of the third party (i.e. omitting names or not disclosing the names or other identifying particulars of the third party); or
- seeking the consent of the third party if practical (e.g. where the third party is easily locatable).

(iv) the Data User is of the view:-

- that the burden or expense of providing access is disproportionate to the risks to the Data Subject's privacy in relation to the personal data

requested via the DAR (e.g. the time, staff and cost that the Data User would need to spend on dealing with the DAR and retrieving the requested data far outweigh the significance of the data to the requestor of the DAR); or

- that the repetitive or trivial nature of the requests would unreasonably burden the operations of the Data User; or

(v) providing access would constitute a violation of a court order; or

(vi) providing access would disclose the confidential commercial information of the Data User, meaning that the provision of the personal data to the Data Subject could possibly harm the competitive position of the Data User. Examples of what amounts to *"confidential commercial information"* include formulations as to the creditworthiness of a customer, or disclosure of the fact that confidential negotiations are ongoing, which might be of value to a competitor of the Data User; or

(vii) access is regulated by another law other than the Act, e.g. the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

1.23 Where an exemption applies to the DAR, a Data User may choose to either refuse the provision of all or some of the personal data requested, depending on the circumstances.

Administrative

1.24 It is recommended that Data Users maintain a record of all DARs that they have received as well the decisions reached in respect of granting or refusing the respective DARs, in order to be able to respond to further queries from the Data Subject or to justify to the Commissioner the reasons for non-compliance with a Data Subject's DAR, in the event of an enquiry or investigation being commenced by the Commissioner.

1.25 It is recommended that Data Users should maintain a record for each DAR with the following information:-

(i) a copy of the DAR;
(ii) a record of the verification of the identity of the requestor;
(iii) copies of all correspondences relevant to the DAR;
(iv) a record of any decision made in relation to the DAR; and
(v) a copy of the personal data that was sent to the Data Subject / requestor in question.

2.0 RIGHT TO CORRECT PERSONAL DATA

2.1 Pursuant to the Access Principle, where personal data of a Data Subject is processed by a Data User and that Data Subject believes that personal data is inaccurate,

incomplete, misleading or not up-to-date, the said Data Subject or requestor may request that one or more corrections be made to his / her personal data.

Ambit Of A DCR

2.2 A DCR may be made in respect of personal data provided by the Data Subject to the Data User during registration and any updates thereto that are currently within the various electronic and physical systems of the Data User.

Format Of A DCR

2.3 A DCR does not have to be in a particular format. However, there are prerequisites that a Data Subject or a request or must fulfil when making a DCR:-

(i) the DCR must be in writing;
(ii) the necessary information and documentation as may be required by the Data User in order to trace and correct the personal data (e.g. name, NRIC / passport number, address, account number) as notified by the Data Subject / requestor;
(iii) the DCR must be specific as to the personal data that is being corrected; and
(iv) relevant certified documentation is to be submitted in order to establish the Data Subject or Relevant Person's right to make a request.

If any one of these prerequisites is not fulfilled, the Data User has the right to return the DCR to the Data Subject / requestor and request for the omitted information / copies to be resubmitted by the Data Subject / requestor.

2.4 In instances where a Data User receives a verbal request for a correction to be made to personal data, the Data User is not required to respond to the request. However, the Data User should guide the Data Subject / requestor on the proper manner of making a valid DCR.

2.5 No fees of are chargeable for making a DCR.

Receipt And Processing Of A DCR

2.6 Data Users are required to provide written acknowledgement of having received a DCR upon:-

(i) confirmation of the identity of the Data Subject / requestor or the submission of relevant certified documentation to establish the requestor's right to make a request on behalf of the Data Subject; and
(ii) the personal data that requires correction being clearly specified.

2.7 In the event the Data Subject's NRIC details do not correspond with the Data Subject's details on record, or the documentation proving the requestor's right to act

on behalf of a Data Subject being insufficient, or the personal data that is need of correction not being clearly specified, Data Users have the right to require the Data Subject or requestor to verify their identity to the Data Users' satisfaction.

2.8 Where the Data User is of the view that it is necessary and/or appropriate (e.g. where there is suspicion of deception / false or misleading information is provided / insufficient documentation provided), it may contact the said Data Subject at his/her last known telephone number / facsimile number / e-mail address in order to confirm that the DCR is legitimate.

2.9 Data Users are required by the Act to comply with the DCR and revert in writing to the person making the DCR within twenty-one (21) days from the date of receipt (i.e. date of acknowledged receipt) of the DCR. Where the initial twenty-one (21) days is insufficient, Data Users are required to communicate with the said Data Subject / requestor informing them of the delay and the required extension, subject to it not being in excess of fourteen (14) days.

2.10 In the event that only some of the personal data can be corrected, Data Users are obliged by the Act to provide the Data Subject / requestor with the sought after personal data to the extent that they are able to do so, whilst informing the said Data Subject / requestor of the efforts being undertaken to provide the balance of the personal data.

Refusal To Comply With A DCR

2.11 Where a DCR is made and the Data User is not satisfied that the personal data in question is inaccurate, incomplete, misleading or not up-to-date, the Data User is required to notify, in writing, the Data Subject concerned of the refusal and the reasons for the refusal no later than twenty one (21) days from the date of the acknowledged receipt of the DCR.

2.12 Pursuant to section 36 of the Act, a Data User has the right not to comply with a DCR where:

(i) the Data User is not supplied with sufficient information as reasonably required (e.g. the name, identification card number, passport number, address, and such other related information as the Commissioner may determine) in order to establish the identity of the Data Subject / requestor, or establish the requestor's connection to the Data Subject; or

(ii) the Data User is not supplied with sufficient information as it may reasonably require in order to ascertain how the personal data in question is inaccurate, incomplete, misleading or not up-to-date (e.g. where the Data User deems the individual as a credit risk based on available data and the individual concerned disagrees with the same but does not provide any other details to the Data User); or

(iii) the Data User is not satisfied that the personal data in question is in fact inaccurate, incomplete , misleading or not up-to-date; or

(iv) the Data User is not satisfied that the correction requested is accurate, complete, not misleading or up-to-date date (e.g. where an individual seeks a change to his / her address but the Data User has grounds to believe the new address provided by the individual to be an attempt in order to avoid the service of a summons on the individual).

2.13 Where appropriate, Data Users may request for supporting evidence from Data Subjects prior to effecting the change requested in their respective DCRs.

2.14 Where the Data User does not comply with a DCR based on any of the reasons provided in 2.12 above, the Data User is required to provide the Data Subject concerned with a written notification of the refusal to comply with the DCR and the Data User's supporting reasons.

Administrative

2.15 It is recommended that Data Users maintain a record of all DCRs that they have received as well the decisions reached in respect of complying or refusing to comply with the respective DCRs, in order to be able to respond to further queries from the Data Subject or to justify to the Commissioner the reasons for non-compliance with a Data Subject's DCR, in the event of an enquiry or investigation being commenced by the Commissioner.

2.16 It is recommended that Data Users should maintain a record for each DCR with the following information:-

(i) a copy of the DCR;
(ii) a record of the verification of the identity of the requestor;
(iii) copies of all correspondences relevant to the DCR;
(iv) a record of any decision made in relation to the DCR; and
(v) a copy of the corrected personal data that was sent to the Data Subject / requestor in question.

3.0 RIGHT TO PREVENT PROCESSING LIKELY TO CAUSE DAMAGE OR DISTRESS

3.1 A Data Subject has the right to request a Data User in writing (referenced in the Act as a "Data Subject Notice") to cease or not to begin processing personal data in relation to the Data Subject, where the processing causes or is likely to cause the Data Subject substantial damage /distress and the said damage/distress is unwarranted.

3.2 However, the Act recognises certain limitations to this right by specifically providing that a Data Subject does not have the right to prevent the processing of personal data where:-

(i) the Data Subject has consented to the processing;
(ii) the processing is necessary:

- for the performance of a contract that the Data Subject has entered into; or
- to take steps at the request of the Data Subject with a view to entering into a contract; or
- for compliance with legal obligations that apply to the Data User, other that a contractual obligation; or
- to protect the Data Subject's *"vital interests"*, which is defined by the Act to mean *"matters relating to life, death or security of a data subject"*.

3.3 Upon receiving a Data Subject Notice, the Data User is required to provide the Data Subject concerned with a written notice within twenty one (21) days of such receipt:-

(i) stating that the Data User has complied with or intends to comply with the Data Subject Notice; or
(ii) if the Data User does not intend to comply with the Data Subject Code, to provide reasons for the decision; or
(iii) 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).

3.4 It is recommended that a Data User takes the following factors into consideration when making a decision on whether to comply with a Data Subject Notice:-

(i) Does the Data Subject Notice set out how the processing is causing damage or distress? The Data Subject will have to provide legitimate reasons. The damage or distress caused will have to be *"substantial"*, before the Data User is obliged to comply.
(ii) Is the damage or distress unwarranted? In the event the Data User feels that any damage or distress caused to the Data Subject is warranted, it is unlikely that the Data User will have to comply with the objection. However, the Data User is required to provide the Data Subject with legitimate reasons for the refusal.

3.5 Where the Data User does not comply with a Data Subject Notice, whether in whole or in part, the Data Subject may submit an application to the Commissioner to require the Data User to comply with the Data Subject Notice.

3.6 Where the Commissioner is satisfied that the application from the Data Subject is justified, the Commissioner may require the Data User to comply with the Data Subject Notice.

4.0 RIGHT TO WITHDRAW CONSENT

4.1 A Data Subject has the right to withdraw his/her consent for the processing of his/her personal data, at any time, by providing the Data User with a written notice.

4.2 Upon receipt and confirmation of a Data Subject's notice withdrawing consent to process his / her personal data, the affected Data User must as soon as reasonably practicable cease to process the Data Subject's personal data, except to the extent where the withdrawal of consent would impinge on the rights and obligations of the Data User under contract or law. Examples of such rights and obligations include:

(i) the right to be paid for the services rendered, e.g. the settlement of any fees stipulated for a minimum term, all bills and overdue payments;
(ii) the right to bring and maintain one or more court actions against the Data Subject;
(iii) the right to mount or continue internal investigations involving any allegations involving the Data Subject;
(iv) the obligation to maintain personal data for such periods as required under applicable legislation; and
(v) the conduct of internal audits, risk management and fulfilment of legal or regulatory reporting requirements.

4.3 For the avoidance of doubt, where a Data Subject has withdrawn consent to process his / her personal data, the Data User has the contractual right to terminate contractual relationship with the Data Subject to the extent the relationship is affected by the withdrawal of the Data Subject's consent.

4.4 By way of example, where the Data User receives a notice withdrawing consent to process a Data Subject's personal data, the Data User may:

(i) commence or follow through on collection of any fees for a stipulated minimum term, outstanding bills and/or overdue payments (if any) or any legal proceedings involving the Data Subject;
(ii) give notice of termination of contract by virtue of the withdrawal of consent to process the Data Subject's personal data;
(iii) remove the Data Subject's personal data from the Data User's electronic and physical systems, as far as reasonably possible;
(iv) remove the personal data from any marketing initiatives or lists of the Data User;
(v) remove the personal data from the control of data processors to the extent applicable; and

(vi) archive the relevant personal data for the applicable statutory period.

4.5 Data Users are required to implement the above measures within a reasonable period of time. Any processing of personal data conducted from the receipt of the notice withdrawing consent to process a Data Subject's personal data until the above measures have been fully implemented shall not result in a breach of the Data Subject's rights.

5.0 RIGHT TO PREVENT PROCESSING FOR PURPOSES OF DIRECT MARKETING

5.1 Pursuant to the Act, a 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/her personal data for purposes of direct marketing.

5.2 For the purpose of the Act, *"direct marketing"* has been defined as *"communication by whatever means of any advertising or marketing material which is directed to particular individuals"*.

5.3 The permitted marketing practices applicable to Data Users are addressed in greater depth in Part 4 of this Code.

5.4 It is recommended that any written request from a Data Subject to cease or not to begin processing his/her personal data for purposes of marketing is to be communicated throughout the organization in order to ensure that the latest instruction of the Data Subject prevails within the organization. A Data Subject's most recent instruction regarding receipt of marketing material shall override his/her previous instructions.

5.5 A Data User needs to comply with the written request within a reasonably practicable time frame. Sufficient time must be allocated for the Data User and its group of companies and/or any related corporations (if any) to update relevant systems and databases to reflect the Data Subject's latest instructions.

5.6 Where Data Subjects make a written request to Data Users stating their choice to receive some direct marketing materials and not others (e.g. direct marketing materials for new communication services and not handset offers), Data Users are permitted to not provide Data Subjects with all direct marketing materials (barring marketing communications that are not specifically targeted as addressed in 4.5 of Part 4), should their systems be incapable of distinguishing between the differing types of services and products so marketed.

PART 6
EMPLOYEES

1.0 POLICIES AND PROCEDURES DEVELOPMENT

1.1 It is recommended that Data Users develop and implement policies and procedures specifying the dos and don'ts and standards expected of employees in their day-to-day work when dealing with Data Subjects' personal data.

1.2 The purpose of developing and implementing such policies and procedures is to prevent data breaches from occurring. An example of a data breach in relation to an employee would involve a situation where an employee of the Data User has access to and discloses personal data outside the authorisation of his/her employment (accessing the calling history of a customer to pry into the personal life of the customer).

2.0 EMPLOYEE TRAINING AND AWARENESS

2.1 Upon the development of policies and procedures, Data Users are required to put in place appropriate training and/or awareness mechanisms for employees to ensure that the employees understand the relevance of policies and procedures to their roles.

2.2 For newly recruited employees, it is recommended that training on personal data protection forms part of their induction into the organization.

3.0 CONTROL SYSTEM

3.1 It is recommended that Data Users put control systems in place to prevent personal data loss in situations where policies and procedures are not followed by employees.

3.2 An effective control system should at cover:-

(i) an employee's access rights to Data Subjects' personal data; and
(ii) the implementation of technical and organizational security measures to prevent personal data breaches by employees.

Access Rights

3.3 In order to mitigate data security risks, it is recommended that employees' access to Data Subjects' personal data is well controlled, wherein employees' are to be provided with access to personal data that is specifically required to do their job.

3.4 It is also recommended that Data Users implement access control policies in order to indicate the various levels of employees that are permitted access, modification and/or deletion rights in relation to different categories of personal data. Refer to 4.6 of Part 3 on access control policy for further details.

Technical and Organizational Security Measures

3.5 The various technical and organizational security measures that may be implemented by Data Users in order to prevent personal data breaches by employees when dealing with Data Subjects' personal data are detailed at 4.6 of Part 3.

PART 7
CODE COMPLIANCE, MONITORING, REVIEW AND AMENDMENT

1.0 CODE COMPLIANCE

1.1 Data Users are required to develop and implement appropriate compliance policies and procedures (compliance framework) in order to ensure compliance with the Act and the Code.

2.0 MONITORING

Monitoring by Data Users

2.1 It is recommended that a Data User regularly monitors its compliance with this Code, the Act, policies and procedures by:-

(i) implementing an internal monitoring framework; and
(ii) conducting self-audits.

2.2 In line with the above, it is recommended that Data Users:

(i) implement a reporting system by key persons within the organization (e.g. the officer(s) responsible for personal data protection, heads of business units and relevant key employees) to the senior management of the Data User, which will look into the status of implementation of the Act, Code, policies and procedures, in order to allow the monitoring of issues, shortcomings or of any progress made; and
(ii) carry out periodic self-audits to identify issues in relation to compliance with the Act, Code, procedures and policies.

2.3 Upon identifying shortcomings and weaknesses in the implementation of the compliance framework, the Data User should ensure that appropriate remedial action is taken as soon as reasonably possible.

3.0 AMENDMENT OF THE CODE

3.1 Amendments to the Code may be made in instances where:-

(i) there are amendments to the Act and Regulations;
(ii) the Commissioner makes amendments on his own accord; and/or
(iii) the CMA Data User Forum makes recommendations for amendments to the Commissioner based on the results of the Code review.

3.2 The CMA Data User Forum must make an application to the Commissioner to make amendments to the Code. The Commissioner shall consult relevant and interested persons such as the Data Users prior to making amendments to the Code.

3.3 Upon approval of the amendments, the Commissioner shall enter the particulars of the amendments in the Register of Code of Practice and make it available to the public.

3.4 All amendments to the Code shall become effective upon registration of the same in the Register of Code of Practice.

4.0 FORUM LIAISON

4.1 The CMA Data User Forum is required to liaise with Data Users at such frequency as may stipulated by the CMA Data User Forum in respect of updates to the Code and other related matters (such as amendments to the Code, developments within the industry, etc.).

4.2 The CMA Data User Forum shall meet with the Commissioner at least once a year in order to discuss the sufficiency of the Code, any proposed amendments to the Act, Regulations or Code, the number and nature of the complaints made to the Commissioner in respect of Data Users, the resolution of the same, and anything else that may be relevant to the Act and its implementation by Data Users.

5.0 CONSEQUENCES OF NON-COMPLIANCE WITH THE CODE

5.1 Pursuant to the Act, a failure by the Data User to comply with the provisions of the Code shall upon conviction be liable to a fine not exceeding one hundred thousand ringgit (RM100,000.00) or to imprisonment for a term not exceeding one (1) year or to both.