Personal Data Protection Code Of Practice

For The Banking And Financial Sector

June 2015

Table Of Contents

Appendix

1. Schedule 11 of the Financial Services Act 2013

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 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 type of conduct that is 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 sectors/industries.

1.4 This Code of Practice is specific to the persons/parties licensed in Malaysia that are engaged in the banking and financial sector of Malaysia, namely all banks and financial institutions licensed under the Financial Services Act 2013, the Islamic Financial Services Act 2013 and the Development Financial Institution Act 2002, and has been developed by The Association of Banks in Malaysia (ABM) as the duly appointed Data User Forum for the banking and financial sector, with the participation and assistance of the Malaysian Investment Banking Association (MIBA) and the Association of Islamic Banking Institutions Malaysia (AIBIM). The Association of Development Finance Institutions of Malaysia (ADFIM) has not responded to the written invitation by ABM to be a party to this Forum.

1.5 Banks and financial institutions that are licensed under the Labuan Financial Services Authority Act 1996 are not considered to be Data Users for the purpose of this Code of Practice and are as such not required to comply with the same. Nevertheless, they may choose to comply with the Code of Practice of their own free will, though the penalties stated herein will not be applicable to them.

2.0 Objectives of the Code

2.1 This Code of Practice ("Code") for the banking and financial sector is intended to:-

(i) set minimum standards of conduct in respect of personal data that are expected of Data Users;

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

(iii) stipulate matters for the consideration of Data Users in order to ensure that the risk to the personal data of Data Subject's is minimised; and

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

3.0 Scope of the Code

3.1 Upon registration of this Code by the Commissioner, the Code shall apply to all licensed banks and licensed investment banks under the Financial Services Act 2013, all licensed Islamic Banks and licensed International Islamic Banks under the Islamic Financial Services Act 2013 and all development financial institutions under the Development Financial Institutions Act 2002.

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

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

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

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

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

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

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

3.3 The individuals identified in 3.2 above, shall collectively be referred to as "Data Subjects".

3.4 In so far as organizations / companies are concerned, where the information of their officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, individual security providers, suppliers/vendors and/or related parties, are provided by the said organizations/companies to Data Users for the purpose of any commercial transaction between these organisations/ companies and 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.

3.5 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, individual security providers, suppliers/vendors and/or related parties, in order to process the said information for the purpose of the commercial transaction between the Data User and the said organizations / companies.

3.6 Other than the above, this Code shall also apply to the relationship between Data Users and the following parties:

(i) third party service providers ("data processors"), for example, where the Data User outsources certain functions (e.g. debt collection, printing of statements) to third parties and provides the said third parties with the relevant personal data of Data Subjects of the Data User; and

(ii) the employees of Data Users, but only in so far as it is relevant to the processing of personal data of Data Subjects by the employees of the Data User.

3.7 With reference to 3.6(ii), CMSRL holders may be hired by Data Users as employees of the Data User, in which case all the provisions of this Code relating to employees will be applicable to the said CMSRL holders. In instances where CMSRL holders are not the employees of a Data User, they shall be treated as independent third parties that are data users in themselves. In the case of the latter instance, their relations with their individual customers shall not fall within the ambit of this Code.

3.8 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 of the Data User; 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.

3.9 This Code shall apply to all personal data and sensitive personal data that are 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".

3.10 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 Association of Banks in Malaysia ("ABM"), as the appointed Data User Forum for the banking and financial sector, shall administer this Code.

4.2 The Commissioner may, upon an application by ABM, revoke, amend or revise this Code, whether in whole or in part, as addressed more detail in section 26 of the Act.

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

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 regulator of the Banking sector (i.e. Bank Negara Malaysia) have 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 be effective upon registration of the Code by the Commissioner in the Register of Codes of Practice.

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 mandatory 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, prosecution or proceeding of any nature, brought against a Data User, whether in court or otherwise, for one or more alleged breaches of the Act and/or Regulations.

PART 2
DEFINITION & INTERPRETATION

1.0 Definitions

1.1 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.

CMSRL holders	means the holder of a Capital Markets Services Representative's Licence issued pursuant to the Capital Markets and Services Act 2007.
Code	means this Code of Practice as may be revised from time to time.
Code of Practice	means this personal data protection code of practice in respect of the persons/parties engaged in the banking and financial sector of Malaysia, namely all banks and financial institutions licensed under the Financial Services Act 2013, the Islamic Financial Services Act 2013 and the Development Financial Institution Act 2002, 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 PDPA.
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 person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data (but does not include a data processor), and for the purposes of this Code, shall specifically refer to the persons identified in 1.4 of Part 1.
Disclose	in relation to personal data, means an act by which such personal data is made available by a data user.
Expression of opinion	means an assertion of fact which is unverifiable or in all circumstances of the case is not practicable to verify.
Opt-in	refers to instances where a Data Subject does not receive services and/or marketing communications of the Data User until such time as the Data Subject makes a positive choice to receive or subscribe to the said services and/or marketing communications.
Opt-out	refers to instances where a Data Subject, based on a pre-existing relationship, automatically receives services and/or marketing communications, until such time the Data Subject takes the positive step of choosing to unsubscribe or not to receive the said services and/or marketing communications.
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 written notice, howsoever described, that a Data User is required to make available to a Data Subject in compliance with section 7 of the PDPA and shall include any privacy statement or privacy policy.
Regulations	refer 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.
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.
Writing / written	includes type writing, printing, lithography, photography, electronic storage or transmission (e.g. via electronic channels) or any other method of recording information or fixing information in a form capable of being preserved (e.g. digital voice recordings).

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 THE 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 with a Data Subject; or

> *Example: Where a Data Subject enters into an agreement with a Data User in order to secure a loan/financing or a credit card, open a savings or current account, open a fixed deposit facility and/or to transmit monies using a money transfer service.*

(ii) the fulfilment of a pre-contractual request of the Data Subject; or

> *Example 1: Where a Data Subject requests that the Data User mail / e-mail one or more financial services product brochures to the Data Subject.*
>
> *Example 2: Where the Data Subject makes an application for a facility with the Data User, and the Data User conducts the necessary pre-contractual credit, anti-money laundering and risk management checks.*
>
> *Example 3: Where an automobile dealer, acting as the agent for the Data Subject, submits a Data Subject's personal data to a Data User in order to obtain the Data User's best rate and terms.*
>
> *Example 4: Where a real estate agent or developer, acting as the agent for the Data Subject, submits a Data Subject's personal data to a Data User, requesting the Data User to contact the Data Subject on available financing packages.*

(iii) in order to comply with any non-contractual legal obligation that the Data User is subject to; or

Example 1: Where the Data User is required to provide personal data of Data Subjects to Bank Negara Malaysia, Inland Revenue or other law enforcement authorities in order to comply with the regulatory reporting requirements of the Anti-Money Laundering and Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

Example 2: Where the Data User is required to provide the personal data of Data Subjects to Bank Negara Malaysia in fulfilment of its obligations under the Financial Services Act 2013 or for the purpose of complying with the regulations or guidelines of Bank Negara Malaysia.

(iv) in order to protect the vital interests of the Data Subject; or

Example: Where the Data User discloses the personal data of the Data Subject to relevant third parties such as the police or to the Data Subject's next-of-kin in matters relating to life, death or security of a Data Subject.

(v) for the administration of justice in accordance with the requirements set out by the law; or

Example 1: Where the Data User is obligated to disclose the personal data to an officer authorized under any written law for the purpose of investigations or prosecution.

Example 2: Where the Data User is obligated to process the personal data of the Data Subject based on a court order (e.g. a garnishee order) served on the Data User.

Example 3: Where the Data User is required to disclose such personal data as necessary in connection with a bankruptcy action.

(vi) for the exercise of any functions conferred upon any person by the law.

Example: Where a Data User is empowered by an Act of Parliament to carry out certain statutory functions.

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 Personal Data Protection Regulations ("Regulations") provide that consent must 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 that are 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,

subject to fulfilment of the requirements of the Regulation 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/continues to use the facility/service of the Data User.

1.7 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.

1.8 Where verbal consent is being recorded, it is recommended that the said consent 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 or an e-mail to the Data Subject).

1.9 For the avoidance of doubt, any consent given to a 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 persons/parties duly empowered by the Data Subject, shall bind the respective Data Subject.

Example: In instances where the Data Subject is a minor, the Data Subject shall be bound by the actions of the Data Subject's guardians.

Processing Personal Data

1.10 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 purpose.

1.11 The criteria set out above are to be read conjunctively and is to be complied with by the Data User over and above the consent requirements of the General Principle.

1.12 In the context of 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.

1.13 As such, in order to comply with the Act, a Data User needs 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.

1.14 The following examples illustrate the above:

Example 1: When filling in an application form to open a personal savings account, the obligatory requirement for the Data Subject to provide the names of the other members of the Data Subject's family to the Data User (other than in the context of providing an emergency contact) would not be relevant to the purpose and would be excessive in relation to the opening or operating a savings account.

Example 2: When filling in an application form, the obligatory requirement for the Data Subject to indicate whether the Data Subject is married or not would not be excessive to the purpose that it is collected for as Data Users are complying with a reporting requirement of Bank Negara Malaysia.

Example 3: When filling in a loan/financing application form, the obligatory requirement for the Data Subject to disclose social demographics (example, marital status, education level and/or race) would not be excessive for the purpose

that it is collected for credit assessment, risk profiling and regulatory reporting.

Example 4: The voluntary provision of personal data indicating the interests and hobbies of Data Subject would not be excessive as the personal data is being provided voluntarily by the Data Subject.

1.15 It is recommended that Data Users:

(i) be clear in application forms, the contractual terms and conditions and/or Privacy Notices about the purpose or purposes for which they collect and hold personal data of a customer; and/or

(ii) indicate in their application forms whether the individual fields of personal data requested are obligatory or voluntary.

2.0 NOTICE AND CHOICE PRINCIPLE

2.1 Data Users are required to make available a written notice, also known as a Privacy Notice, to Data Subjects prior to or as soon as possible after the collection of 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 that particular Data User. It is a general non-exhaustive statement about the privacy practices of that Data User that should result in individuals having greater confidence in how Data Users 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 a subsidiary within a larger group of companies, 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.

2.5 In addition to the above, Data Users may also address matters such as the security and retention of personal data of Data Subjects in order to provide the Data Subject with a more complete idea as to the overall protection of his/her personal data. However, this is not a requirement of the Act or the Regulations and each Data User will need to determine whether or not to incorporate the same within its Privacy Notice.

2.6 The Privacy Notice needs to be provided in Bahasa Malaysia and English languages. The provision of the Privacy Notice in only one language will not fulfil the requirements of the Notice and Choice Principle.

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.

> *Example: The provision of an opportunity to view or read the applicable Privacy Notice via a website address/link, prior to the submission of a web form containing the personal data of the Data Subject.*

2.8 In the case of Data Subjects whose personal data was collected prior to the enforcement of the Act, the Notice and Choice Principle requires Data Users to provide Data Subjects with a Privacy Notice prior to the Data User:

(i) using any part of the said personal data for a purpose other than the purpose it was collected for in the first place (for instance when intending to market insurance services to loan/financing applicants); or

(ii) disclosing any part of the said personal data to any third party (including the third parties that have been indicated within the Data User's Privacy Notice).

2.9 The recommended course of action in instances where personal data was collected prior to the enforcement of the Act is to communicate the Privacy Notice to all Data Subjects, whether existing or new. This recommendation is made in order to avoid the administrative burden involved in keeping track of the purposes that it was originally collected for, and keeping track of its potential disclosure to third parties.

Modes Of Communicating The Privacy Notice

2.10 Data Users may communicate their Privacy Notices to Data Subjects by one or more of the following methods:

(i) by posting a printed copy of the Privacy Notice to the last known address of the Data Subject; or

(ii) by posting the Privacy Notice on the website(s) of the Data User; or

(iii) by issuing a SMS 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

(iv) 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

(v) by issuing an electronic message to Data Subjects providing a website address/link to the Data User's Privacy Notice and/or telephone number to contact for further information via such other electronic channels utilised by Data Users; or

(vi) 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

(vii) by prominently displaying a summarised version of the Privacy Notice at the premises of the Data User's place of business (e.g. at the notice board, at the counter desk that Data Subjects come to and/or at a prominent location in the banking hall), and making available the full Privacy Notice either upon a request being made at the counter or to the personnel of the Data User; or

(viii) by displaying a message on the screens of Automated Teller Machines (ATM) / Cash Deposit Machines (CDM) with a website address/link to the Privacy

Notice, a telephone number to contact for further information and/or stating that the Privacy Notice is available at the branch of the Data User; or

(ix) by inserting a statement in application / registration forms referencing the Privacy Notice, which may be accessed at a given website address/link, or by making a request to personnel of the Data User, or by calling a telephone number provided in the application / registration form; or

(x) by printing out copies of the Privacy Notice and providing it to Data Subjects at the Data User's premises; or

(xi) any other mode of communicating the Privacy Notice as approved by the Commissioner or that serves to bring the Privacy Notice to the attention of the Data User.

2.11 In selecting the mode of communication of the Privacy Notice, Data Users need to determine the most appropriate ways of reaching as many of their clientele as possible, especially bearing in mind that some of them may not be computer literate. As such it is recommended that Data Users utilise a mix of the modes of communication as indicated above in order to ensure that the Privacy Notice is communicated to as many Data Subjects as possible.

2.12 The Regulations require Data Users to maintain records of having communicated the Privacy Notice to its 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.

Example 1: Where the Privacy Notice is communicated to Data Subjects by prominently displaying a summarised version of the Privacy Notice at the premises of the Data User's place of business and making available the full Privacy Notice at the counter, the production of the summarised Privacy Notice and the full Privacy Notice, shall be sufficient to prove that the Privacy Notice has been communicated to Data Subjects.

Example 2: Where the Privacy Notice is communicated by e-mail to Data Subjects, the production of the relevant e-mail referencing the Privacy Notice, the Privacy Notice in itself and the provision of the names of Data Subjects that the e-mail was sent to, shall be sufficient to prove that the Privacy Notice has been communicated to Data Subjects.

Example 3: Where the Privacy Notice is communicated by SMS to Data Subjects, the production of the text of the relevant SMS referencing the Privacy Notice, the Privacy Notice in itself and the process for the communication of the SMS to Data Subjects, shall be sufficient to prove that the Privacy Notice has been communicated to Data Subjects.

Acceptance Of Privacy Notice

2.13 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 2.10 above, the Privacy Notice shall be deemed to have been communicated afresh to the Data Subject.

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

3.0 DISCLOSURE PRINCIPLE

3.1 The term *"disclosure"* has not been defined by the Act and as such should be interpreted utilising the normal dictionary meaning.

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.

3.3 The Disclosure Principle is closely tied to the Notice and Choice Principe in that the purpose declared by the Data User for the collection of the Data Subject's personal data is of central importance.

Permitted Disclosures

3.4 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

> *Example: Where a Data Subject provides his/her information for the purpose of making a credit card application, and as a part of the process of approving and providing the credit card to the Data Subject, the Data Subject's personal data needs to be provided to one or more third parties to whom the Data User has outsourced parts 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

Example: Where the Data Subject defaults on payments under a loan/financing agreement, leading the Data User to appoint a solicitor / debt collection agent to recover the amounts outstanding. Where the solicitor's / debt collection agent's letters of demand are returned due to the Data Subject having moved, the solicitor / debt collection agent may make their own inquires as to the Data Subject's whereabouts without disclosing details of the claim against the Data Subject. The disclosure of such limited personal data while making inquiries is permissible as it is directly related to the primary purpose of providing the Data Subject with the said loan/financing.

(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 (without derogating from any laws, regulations, standards, guidelines and/or obligations applicable to Data Users).

Example: Third parties that may be identified within the Privacy Notice are (a) organizations and agents of the Data User that assist in fulfilling the transactions requested by the Data Subject, (b) parties authorised by the Data Subject (e.g. auditors, financial advisers), (c) merchants and strategic partners of Data Users, and/or (d) credit reference agencies.

3.5 Data Users are to note that the Regulations require Data Users to maintain a listing of the disclosures made to the various classes / categories of third parties as detailed in their respective Privacy Notices.

3.6 Other than the disclosures permitted based on the Privacy Notice as detailed in 3.4, 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

Example: Where the Data User realises that consent is required and proceeds to write to the Data Subject requesting for such consent, which is then provided by the said Data Subject.

(ii) the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or

Example 1: Where there has been a security breach within the Data User's organization and the Data User proceeds to disclose the information to a forensics specialist for an internal investigation.

Example 2: Where personal data is released to the police for the purpose of their criminal investigations.

Example 3: Where information regarding individuals suspected of fraud, or abetting the same, is disclosed to one or more Data Users in order to prevent and/or detect future attempts to defraud the Data User.

(iii) the disclosure is required or authorized by or under any law or by the order of a court; or

Example 1: Where certain disclosures of information (which may include personal data) are authorised or permitted by an Act of Parliament, e.g. the Financial Services Act 2013. The said Act states that information relating to the affairs or accounts of any customer of a financial institution shall not be disclosed to another person, other than in certain circumstances as detailed in Schedule 11 of the said Act, which is annexed to this Code as Appendix 1. By way of illustration, Schedule 11 permits the disclosure of information regarding the affairs/accounts of a customer (i) to a person appointed as the legal representative of a customer in instances where the customer is incapacitated, or (ii) to persons named in an order of Court served on the financial institution requiring such disclosure.

Example 2: Where disclosures are made to authorities having jurisdiction over the Data Users or its group members and/or service providers appointed by the Data Users or its group members in meeting obligations, requirements or arrangements, whether compulsory or voluntary to comply with, or in connection with any law, regulation, judgment, court order, voluntary code, sanctions regime, within or outside Malaysia existing currently and in the future.

(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

Example: Where an injunction is served on the Data User in respect of a Data Subject's account, requesting the Data User to disclose personal data of the Data Subject.

(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

Example: W*here the Data Subject is medically incapacitated and the Data*

User discloses the Data Subject's personal data to his immediate next of kin subject to an indemnity agreement being entered into.

(vi) the Minister determines the disclosure as being justified in the public interest.

3.7 In respect of 3.6(ii) above, Data Users should be aware that in instances where personal data is disclosed for the prevention or detection of crime or for purposes of investigation (whether internal or external), the Act exempts Data Users from providing the Data Subject with any information pertaining to the said disclosure even where a data access request is filed with the Data User.

3.8 For the sake of completeness, Data Users are to note that the processing of personal data in certain instance 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 journalistic, literary or artistic purposes.

3.9 Apart from disclosures pursuant to the circumstances as detailed above, or as may otherwise be permitted by applicable laws, regulations and/or guidelines, no other disclosures are permitted under the Act.

Requests For Personal Data

3.10 Data Users may receive requests from third parties for the disclosure of personal data of Data Subjects. When they do, Data Subjects will need to determine whether:

(i) the intended disclosure would fall within the ambit of the permitted disclosures as stated in the Privacy Notice as detailed in 3.4 and 3.6; or

(ii) the intended disclosure is otherwise exempted under the Act as detailed in 3.8.

3.11 In order to streamline the obligations of Data Users vis-à-vis disclosure, it is recommended that each Data User put in place a disclosure policy (or incorporate the same within their relevant internal documentation) detailing the various instances where disclosure is permitted or otherwise, as well as the process and procedures that need to be adhered to when dealing with third party requests for disclosure of personal data.

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 Data Users within the banking and financial sector are required to comply with Bank Negara Malaysia's guidelines on security as a condition of their banking licenses under the Financial Services Act 2013 and the Islamic Financial Services Act 2013. Further, the employees of Data Users are bound by the rules on secrecy in the Financial Services Act 2013 and the Islamic Financial Services Act 2013. As such, Data Users are in most, if not all, respects already compliant with the Security Principle as embodied in the Act.

4.5 In complying with the Security Principle, it is recommended that Data Users assess, as and when necessary, whether their existing security policies or such other internal documentation as may be applicable, address the following key factors:

(i) Organizational Security

(a) Data classification
(b) Access control
(c) Bring Your Own Devices (BYOD) Confidentiality
(d) Supervision/monitoring of personnel

(ii) Technical Security

(a) Physical document security
(b) Physical access to IT facilities
(c) Physical access to IT systems and communications equipment
(d) Access authorisation systems
(e) Limiting access to technologies that may be used to disseminate personal data
(f) Back-ups
(g) Anti-virus and anti-malware software
(h) Encryption and other forms of securing access

4.6 Additionally, Data Users are required to have in place disaster recovery plans and business continuity plans in order to effectively secure the personal data of Data Subjects against disasters and business interruption which Data Users may experience. Data Users are required to test their disaster recovery and business continuity plans from time to time and maintain records of the same.

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 and debt collecting agents for the purposes of debt recovery) 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 The range of technical and organizational security measures that Data Users may require data processors to provide vis-à-vis personal data, are briefly identified in 4.5 above. In practice, it is more likely that Data Users will need to raise and negotiate the technical and organizational security measures required by the Data User 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 agreements with data processors (whether in the form of contracts or letters of engagement or otherwise) addresses the following matters:

(i) the data processor's agreement 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 agreement 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 agreement 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 ascertain the technical and organizational security measures deployed by the data processor (e.g. by way of an on-site audit, issuing a questionnaire or securing a declaration) 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 must 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 regulators of the banking and financial sector, and/or any security standard(s) (or their equivalent) as may be prescribed by 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.

5.2 This requirement applies to both physical and electronic copies of documents containing personal data.

To Be Read Together With Other Applicable Acts

5.3 While the Act appears to be clear as to the duration that personal data may be retained for, namely:

(i) that personal data processed for a particular purpose, is not to be retained by the organization for longer than is necessary for the fulfilment of the said purpose; and

(ii) that when the personal data is no longer needed for its purpose, the Data User is required to destroy or permanently delete the personal data,

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, the Limitation Act 1980, the Limitation Ordinances of Sabah and Sarawak or the Anti-Money Laundering and Anti-Terrorism Financing Act 2001. The Act and such other applicable legislation must be read together.

Applicable Retention Periods

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

5.5 However, in the specific case of rejected applications for any banking facilities (e.g. applications for loans or hire purchase), Data Users are permitted to maintain said rejected applications for up to seven (7) years, after which Data Users must delete the said rejected applications, unless:

(i) the Data User can establish sufficient grounds to continue retaining the said rejected applications; or

(ii) the Data User is required by its regulators (e.g. Bank Negara Malaysia) to continue maintaining the rejected applications; or

(iii) the Data User is required by law to continue maintaining the rejected applications for a duration longer than seven (7) years.

5.6 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, it is recommended that Data Users identify all applicable retention periods and ensure that they are reflected in the appropriate retention policy(ies) of the Data User.

5.7 For the purposes of this Code, the Retention Principle does not apply to backup media and/or electronic archives, 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

5.8 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.

5.9 In respect of physical / paper based personal data, the disposal of the personal data by throwing it into a waste paper basket does not suffice to constitute *"destruction"* as there is no guarantee as to what will occur to the discarded personal data. Data Users will need to utilise proper means to *"destroy"* the personal data, e.g. using a paper shredder or incinerating the discarded personal data. In terms of personal data stored on an electronic medium, the *"permanent deletion"* of the personal data will require the electronic media (e.g. hard drive or a USB thumb drive) to be wiped clean once the data has been deleted. Data Users are to note that deletion alone is not sufficient to remove the personal data from the electronic media.

5.10 For the avoidance of doubt, Data Users are to note that personal data that are physically archived are still subject to the provisions of the Act and will continue to

remain so until they are destroyed /permanently deleted or anonymized. Bearing in mind the volume of records containing personal data that are required to be destroyed / permanently deleted or anonymized, Data Users respective retention policies shall address the restricted access to and the destruction of such personal data.

5.11 The destruction of personal data itself falls under the definition of *"processing"* under the Act, and as such, the destruction of data should also be in compliance with other relevant principles of the Act. For example, where the destruction of personal data belonging to the Data User is carried out by a data processor, the Data User is to take practical steps pursuant to the Security Principle in order to ensure that personal data is destroyed and is not misused or mishandled by the Data Processors.

5.12 As an alternative to destroying or permanently deleting the personal data, Data User may wish to 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

5.13 Data Users must also comply with any retention standards as may be set out by the Commissioner from time to time.

5.14 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 regulators of the banking and financial sector, and/or any retention standard(s) (or their equivalent) as may be prescribed by 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 as well as the directly related 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

unfavourable decision in relation to a Data Subject's application for a credit card);

(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 that the personal data of the Data Subject should reflect the latest verified information in respect of the Data Subject, for example a change of address or capturing a loan/financing instalment payment made 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. For example, where personal data is maintained by the Data User for the purpose of issuance of monthly credit card statements, it would be reasonable for the Data User to ensure that the personal data that it has collected remains correct and that it is kept up-to-date. However, where the personal data is collected for the purpose of a one-off transaction and the record of the same is being maintained for regulatory reporting purposes, it would be unreasonable to expect the Data User to continue ensuring that the address of the Data Subject is kept up-to-date.

6.4 Data Users would need to assess the personal data of Data Subjects that they are currently processing as well as other relevant factors (e.g. the purposes of the processing being carried out and the frequency of communications with the Data Subject), in order to determine the specific measures that need to be implemented in order to comply with the Data Integrity Principle.

6.5 This Code does not specify the means of complying with the Data Integrity principle and leaves it to the discretion of Data Users. Nevertheless, the adoption of the following steps may be considered by Data Users:

(i) provision of personal data update forms at branches of the Data User and at/via other points of contact with Data Subjects; and/or

(ii) availability of a call centre in order for Data Subjects to update their personal data.

6.6 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.

6.7 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 provide complete and accurate information and 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.

6.8 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.

6.9 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 first became a Data Subject of 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 application for a loan/financing was wrongfully rejected 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

6.10 Data Users must also comply with any data integrity standards as may be set out by the Commissioner from time to time.

6.11 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 regulators of the banking and financial sector, and/or any data integrity standard(s) (or their equivalent) as may be prescribed by 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 Relevant Person's identity, establish the identity of the Data Subject, or establish the Relevant Person'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 Relevant Person); or

(iv) are of the view 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 the Relevant Person; 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 access to the said personal data is regulated by another law.

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 BANKING AND FINANCIAL SECTOR

1.0 PERSONAL DATA

1.1 The banking and financial sector 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 considered as personal data due to the data not meeting one or more requirements of the Act.

1.2 The following listings are provided in order to indicate the types of data which fall within the definition of *"personal data"* (as contained in section 4 of the Act) for the purposes of the Act, as well as the types of data that fall outside the ambit of the Act and are as such not considered to be *"personal data"*.

(i) Personal data:

- The personal particulars of an individual, whether obtained from the individual directly or derived from other any other data that the Data User has access to
- The details an individual provides on an application to obtain a loan/financing, credit card, or other financial product or service
- The details of an individual's account balance information, credit history, income and spending patterns
- The details of an individual's ownership of properties or assets
- The employment information of an individual
- The details of an individual obtained through credit evaluation or assessment
- The details of individuals and their browsing session(s) captured via the use of website cookies
- The details of the individual as listed within a manual or electronic database

(ii) Not personal data:

- Data relating to organizations (as referred to in 1.3 below)
- Data relating to deceased individuals
- Data pertaining to individuals that have been aggregated and/or anonymised in such a manner as to render the individual non-identifiable

1.3 In so far as organizations / companies are concerned, where the information of their officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, individual security providers, suppliers/vendors and/or related

parties, are provided by the said organizations/companies to Data Users for the purpose of any commercial transaction between these organisations/ companies and 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, individual security providers, suppliers/vendors and/or related parties, in order to process the said information for the purpose of the commercial transaction between the Data User and the said organizations / companies.

1.5 However, in instances where the Data User utilises the data of the officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, individual security providers, 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 credit card facilities in his personal capacity), the said officers, employees, authorised signatories, directors, individual shareholders, individual guarantors, individual security providers, suppliers/vendors and/or related parties shall be considered to be Data Subjects and shall be entitled to rights under the Act.

1.6 Where Data Users make available application forms of third party service providers (e.g. insurance / takaful providers) at their premises and do not in any way process the personal data of Data Subjects on the completed third party application forms (e.g. where the completed application form is inserted into a post box accessible to the third party service provider only), the mere provision of such application forms shall not fall within the ambit of 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 an insurance product to Data Subjects includes the collection of personal health or medical history of a customer. Where this is done, the Data User concerned would be in possession of sensitive personal data pertaining to the health of the customer. In these instances, the *"explicit consent"* of the customer is required under the Act.

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 legal rights.

2.4 In the context of the banking and financial sector, 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 accounts. Frequently, this takes the form of:

(i) photocopying the NRIC, returning the NRIC itself to the customer and retaining the copy of the NRIC; and/or

(ii) electronically reading the chip on the NRIC, returning the NRIC to the customer and retaining the information obtained from the chip in an electronic format.

In the case of the latter instance, where all the information available on the chip of the NRIC is captured and retained in the system(s) of Data Users, information relating to the religion of the customer will be captured by the said system(s). 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 PDP Regulations provide that any *"consent"* obtained must be capable of being *"recorded"* and *"maintained"*. As such, it may be presumed that at the minimum, 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 his/her sensitive personal data. Bearing in mind the stipulations of the PDP Regulations in relation to consent (i.e. that consent must be capable of being *"recorded"* and *"maintained"*), it is recommended that any verbal explicit consent given by the Data Subject should be recorded, for example via an audio recording, 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. submitting the Data Subject's NRIC for reading at the stage of applying for a facility / service / product of the Data User); 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 consent to the processing of his/her personal data, e.g. by way of a signature or tick of the Data Subject indicating his/her consent.

> *Example: Where a Data Subject fills up an application form when applying for an insurance product with the Bank, the customer provides his/her explicit consent by signing the application form or ticking the relevant part of the application form, thereby enabling the Data User to process his/her Sensitive personal data (e.g. the medical history of the customer).*

3.0 PRE-EXISTING DATA

3.1 This Code shall apply to all personal data and sensitive personal data that are 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".

3.2 Notwithstanding the foregoing paragraph:

(i) where the personal data / sensitive personal data relates to inactive, closed, dormant or archived 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 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"* means any form of unsolicited communication including but not limited to personal interaction, door-to-door sale calls, post, telephone, fax, e-mail, SMS, or via other electronic channels;

(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 targeted 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 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. For the avoidance of doubt, communicating with Data Subjects in respect of the renewal of services / facilities (e.g. the renewal of an annual automobile insurance policy) already subscribed to shall not be considered to be direct marketing.

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** current account customers of a Data User) of a Data User, will not be considered direct marketing for the purposes of this Code.

Example 1: Including marketing/promotional inserts in bank statements issued to all current account customers of a Data User (i.e. to individuals, companies, partnerships), shall not amount to direct marketing for the purposes of the Act.
Example 2: Including promotional banners on the website of the Data User which are visible to all internet banking customers of the Data User (i.e. to individuals, companies, partnerships), shall not amount to direct marketing for the purposes of the Act.

Example 3: Directing promotional material to selected Data Subjects with a current account balance of more than RM1,000,000 shall amount to direct marketing for the purposes of the Act.

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.

Consent And Notice

4.7 Data Users are governed by Bank Negara Malaysia's mandated requirements under the Product Transparency & Disclosure Guidelines ("PTDG") in relation to disclosing personal data to:

(i) companies within the Data User's group of companies for the purpose of cross-selling; and

(ii) companies outside of the Data User's group of companies for the purposes of marketing and promotions.

4.8 In cases where the personal data collected is to be disclosed to other companies within the Data User's group of companies for the purpose of cross-selling, Data Users are to be guided by Bank Negara Malaysia's PTDG, which provides:

The FSP wishing to share customer information with other companies within the financial group must inform the customer to whom the information may be disclosed to and the purpose for such disclosure. However, the FSP shall not share the information of any customer who has objected to such disclosure for purposes of cross-selling. For new customers, the FSP must give the customer the opportunity to "opt-out" for such disclosure for purpose of cross-selling. For existing customers, the FSP should communicate on the discretion provided to the customer to "opt-out" and provide the means for customers to do so.

**FSP has been defined by the PTDG as "financial service providers".*

4.9 In cases where the personal data collected is to be disclosed to merchants and/or strategic partners of the Data User for the purpose of direct marketing, Data Users are to be guided by Bank Negara Malaysia's PTDG, which provides:

The FSP wishing to share customer information (excluding information relating to the affairs or account of customer) with third parties, such as strategic alliances for marketing and promotional purposes, must obtain the expressed consent of the customer. Towards this end, the FSP must give the customer the opportunity to

"opt in" for such disclosure of the information to the parties specified by the FSP. For avoidance of doubt, in the event that a customer who has "opted in" subsequently communicates his objection to sharing his information with third parties, such communication shall supersede any earlier consent given to FSP.

4.10 As such, for the purposes of this Code and based on the requirements of Bank Negara Malaysia's PTDG, it shall be sufficient for Data Users to notify their Data Subjects, via their respective Privacy Notices, of marketing activities conducted by:-

(i) the Data Users themselves (and provide that Data Subjects may opt-out of such direct marketing activities);

(ii) companies within the Data User's group of companies for the purpose of cross-selling (and provide that Data Subjects may opt-out of such cross-selling marketing activities); and

(iii) companies outside of the Data User's group of companies (e.g. merchants and strategic partners) for the purposes of marketing and promotions (and provide that unless Data Subjects opt-in to such marketing activities, they will not receive such marketing materials).

4.11 Data Users communicating advertising or marketing material directed to particular Data Subjects, through the utilisation of the 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),

are required to either have already notified the Data Subjects of the same via their respective Privacy Notices (as detailed in 4.12 below), or in cases where their Privacy Notices are silent as to the issuance of such advertising or marketing material, are required to obtain the consent of the Data Subject prior to commencing direct marketing.

4.12 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. 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.

4.13 Data Users must provide such notifications to Data Subjects via their respective Privacy Notices which need to be communicated 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

4.14 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 or by referral from Data Subjects themselves.

4.15 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.

4.16 Data Users may do so:

(i) in the case of commercial arrangements with third parties, 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; and

(ii) in the case of Data Subjects that are customers of the Data User, by obtaining warranties (whether written or verbal) from the Data Subjects that they have secured the necessary consent from the said individuals in order for the Data User to market their products / services to the said individuals.

4.17 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.

Appointment Of Marketing Agents

4.18 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, the Data Users are to impose certain requirements upon the Data Processor as laid out in 4.19 below.

4.19 The Data User shall on a reasonable efforts basis ensure that any processing of personal data by the Data Processor takes place subject to a contract between the Data User and the Data Processor 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 Data Processor;

(iii) the technical and organizational security measures governing the processing to be carried out;

(iv) steps to ensure compliance with those measures (e.g. the conduct of paper based audits); and

(v) the deletion, destruction and/or the return of the personal data upon completion or termination of the contract.

Data Subject's Right To Refuse Direct Marketing

4.20 As stated in 4.12(iii), at a minimum, Data Users need to provide all Data Subjects with the right to refuse the use of their personal data for direct marketing purposes.

4.21 Such requests may be made:-

(i) via the initial application form when signing up for new products/services through an opt-out of direct marketing tick-box; or

(ii) via a separate form made readily available to the Data Subject by the Data User; or

(iii) via such other mode of communication as notified by the Data User or as may be acceptable to the Data User,

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

4.22 A systematic approach is to be adopted by the Data User to effectively comply with a Data Subject's request to cease direct marketing. Data Users need to maintain a system, database, procedure or process whereby such requests are captured. The said system, database, procedure or process will serve as a point of reference in the future to ensure that marketing materials are not sent to the Data Subjects listed therein.

4.23 It is recommended that Data Users develop policies and procedures for its marketing staff to adhere to in relation to accessing and updating the said system, database, procedure or process and complying with Data Subjects' requests.

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

4.24 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.

4.25 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 (e.g. application for a loan/financing) 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 (e.g. application for credit cards/loan/financing facilities);

(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 (e.g. obtaining the consent of Data Subjects to the CRA's release of the of the Data Subjects' credit report to the Data User) within the terms and conditions governing the Data User's relevant services / facilities.

5.5 Data Users may also insert tick boxes into relevant application forms requesting Data Subjects to consent and authorize Data Users to conduct credit checks with any CRAs and corporations set up for the purpose of collecting and providing consumer credit information.

6.0 PERMITTED DATABASES

6.1 Pursuant to section 45(2)(a)(i) of the Act, Data Users are permitted to maintain one or more databases (or their equivalent, whether electronic or paper based) of individual applicants and customers that have attempted to obtain services, or have obtained services, from Data Users based on inaccurate and/or fraudulent information, in order to detect future applications from said individuals and to mitigate the risk of fraud to Data Users.

6.2 Each Data User is permitted to maintain its own database of individual applicants and customers that have attempted to obtain services, or have obtained services, from Data Users based on inaccurate and/or fraudulent information and may disclose the information to any other Data User and/or receive such information from other Data Users for the purpose of the detection of fraud.

6.3 Further to the above, Data Users are permitted to process information from the Malaysia Department of Insolvency as to individuals that are bankrupt and therefore not qualified to open or maintain accounts/facilities with Data Users.

6.4 Data Users are also permitted to maintain lists of individuals that have been sanctioned by local and/or foreign regulators, governmental authorities and international organizations in order to avoid breaching any laws, regulations or treaties that are applicable to Data Users.

6.5 Data Users are permitted to reference the said databases / lists upon applications for banking and financial services / facilities being lodged with Data Users and in the management and operation of their respective banking businesses.

7.0 CONTACTING THE DATA SUBJECT

7.1 In the management and operation of the Data Subject's accounts / facilities with the Data User, occasion may arise where the Data User needs to get in touch with the Data Subject via the telephone.

7.2 Where the Data User contacts the Data Subject on the Data Subject's given telephone numbers and the call is received by someone other than the Data Subject, it is permissible for the Data User to inform the said recipient of the call of the identity of the Data User, when would the Data Subject be available and to state that the Data User will call back later.

7.3 Data Users are not permitted to disclose any other details regarding the Data Subject, the Data Subject's accounts / facilities with the Data User, and/or the status of the said accounts / facilities, to the recipient of the call.

8.0 CERTIFICATE OF REGISTRATION

8.1 Data Users are required by the PDP Regulations to display:

(i) the original Certificate of Registration issued by the Commissioner pursuant to the Act at 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,

(hereinafter collectively referred to as "Certificates").

8.2 Data Users may display the Certificates in their respective banking halls, 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.

8.3 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.

9.0 PHOTOGRAPHY DURING CORPORATE EVENTS

9.1 Photos and images of individuals taken by or for Data Users fall within the ambit of the Act where the individuals are identifiable.

9.2 In instances where Data Users organise an event at which individuals will be photographed and such photographs published in the publicity materials, internal magazines and/or the intranet of Data Users, it is recommended that Data User adopt the following measures:-

(i) if the event is by invitation, the invitation card clearly states that photographs of attendees will be taken at the event and that the images may be used for publication by the Data User; or

(ii) if the event is open to the public, an obvious notice is put up at the entrance or reception of the event venue to inform attendees that photographs of attendees will be taken at the event and that the images may be used for publication by the Data User.

10.0 TRANSFER OF PERSONAL DATA ABROAD

10.1 The Act prohibits the transfer of personal data outside of Malaysia unless the transfer is to a country with sufficient data protection laws, as specified by the Minister in a Government Gazette, which will be based on the Commissioner's recommendation to the Minister.

10.2 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 where a customer gives the Data User an order to transfer money into the account of a third party); 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.

10.3 Based on the above, it is recommended that Data Users:

(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 10.4 below.

10.4 It is recommended that Data Users use their reasonable efforts to secure the following representations and warranties from the said recipient of the personal data:

(i) to provide all information and cooperation regarding the processing of personal data as the Data User may reasonably require to enable the Data User's compliance with the Act;

(ii) to carry out the processing of the Data Subject's personal data only as necessary to fulfil its contractual obligations to the Data User;

(iii) not to divulge the whole or any part of the Data Subject's personal data to any person, except to the extent necessary to fulfil its contractual obligations to the Data User;

(iv) to implement and maintain the necessary technological and organizational security measures, and provide details of the same to the Data User if requested, in order to protect the Data Subject's personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

(v) not to retain the Data Subject's personal data for longer than is necessary for the fulfilment of its contractual obligations to the Data User;

(vi) to permit the Data User and/or its representatives (subject to agreeable confidentiality undertakings), to conduct either physical or paper-based audits of the recipient's personal data processing facilities and activities in order to ensure compliance with the Act if necessary; and

(vii) to return or destroy all of the Data Subject's personal data to the Data User upon the end of the relationship/the recipient's business goes out of business/upon request.

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.

Ambit Of A DAR

1.2 A DAR may be made in respect of personal data that is currently within the various electronic and physical systems of the Data User as provided by the Data Subject to the Data User.

1.3 Any expressions of opinion held by a Data User may also be the subject of a DAR.

> *"expression of opinion"* includes an assertion of fact which is unverifiable or is impracticable to verify under the available circumstances. Examples as to what amounts to an *"expression of opinion"* include an internal assessment of the risk profile of a Data Subject, or an entry into the Data User's Customer Relationship Management system indicating a personal opinion regarding the said Data Subject.

1.4 However opinions issued or kept solely for evaluative purposes or which discloses the confidential commercial information of the Data User shall not be subject to a DAR.

> Examples of what constitutes an expression of opinion issued or kept for evaluative purposes includes opinions in credit papers, in-house /external legal opinions, compliance, audit, fraud or other investigative opinions issued for purposes which include risk management, deciding on the credit worthiness of a Data Subject and whether any contract with the Data Subject should be continued, modified or terminated.

1.5 Data Users are required to ensure that the personal data 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 utilizing 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

must 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 electronic 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 1.2 and 1.3 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.

1.10 A DAR may also be made on behalf of the Data Subject by the following persons:

(i) in the case of a Data Subject who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the data subject; or

(ii) in the case of a Data Subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorized in writing by the data subject to act on behalf of the Data Subject; or

(iii) in any other case, a person authorized in writing by the Data Subject to make a data access request, data correction request, or both such requests, on behalf of the Data Subject,

(collectively referred to as the "Relevant Persons").

Format Of A DAR

1.11 A DAR does not have to be in a particular format. However, there are prerequisites that a Data Subject or a Relevant Person must fulfil when making a DAR:-

(i) the DAR must be in writing (as defined in Part 2);

(ii) the payment stipulated by the Regulations needs to be enclosed together with the DAR, except where it is waived by the Data User;

(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 Relevant Person's right to make a request.

If any one of these prerequisites is not fulfilled, the Data User should return the DAR to the Data Subject / Relevant Person and ask for the omitted information / payment / copies to be resubmitted by the Data Subject / Relevant Person.

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

1.13 Data Users cannot make it mandatory that such standardised forms are to be used in order to make a DAR. Any request in writing lodged with a Data User, whether in the form of a letter, e-mail or a memo, will qualify as a valid DAR, as long as the minimum criteria specified in 1.11 are fulfilled.

1.14 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 / Relevant Person on the proper manner of making a valid DAR and provide whatever assistance as may be required by the Data Subject / Relevant Person to make a DAR.

Receipt And Processing Of A DAR

1.15 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 / Relevant Person;

(ii) submission of relevant certified documentation to establish the Relevant Person'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.

1.16 The Data User will apply its identity verification processes in order to verify that the DAR is from the Data Subject or from a Relevant Person. The Data User may reject the request if the Data User is not able to verify the identity of the person making the request. The Data User is required to state the reason for the rejection to the Data Subject / Relevant Person.

1.17 Where the Data User is unclear as to the specific personal data that is being sought by the Data Subject / Relevant Person, the Data User may request (depending on the Data Users respective policies) for further information, e.g. account numbers, dates of specific transactions, 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 / Relevant Person in question, except for instances in which such DARs may be rejected as provided for in the Act and further elaborated 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 / Relevant Person 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 requested and stated in the DAR can be located, Data Users are obliged by the Act to provide the Data Subject / Relevant Person with the sought after personal data to the extent that they are able to do so, whilst informing the said Data Subject / Relevant Person of the efforts being undertaken to provide the balance of the personal data.

1.21 In relation to the communication of video and audio personal data to Data Subjects / Relevant Persons who have made a DAR, Data Users may utilise the following means of communication as may be available to them:

(i) audio recordings may be communicated as written transcripts or provided in audio form (e.g. .wmv or mpeg); and/or

(ii) video recordings (inclusive of CCTV images) may be communicated as a chronological set of image captures which are then printed, or as an edited video recording where all other persons' identities have been removed or masked.

Refusal To Comply With A DAR

1.23 A Data Subject has the right to lodge a complaint with the Commissioner in the event a Data User does not comply with a DAR. However, the Act recognises that Data Users may legitimately refuse to comply with a DAR in some circumstances as detailed in section 32 of the Act.

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

1.25 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 / Relevant Person, or establish the Relevant Person'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 (e.g. where a Data Subject of a bank has requested access to his/her CCTV images but has not identified the branch visited and the date of the visit) or in the Data Subject's request for audio recording of the Data Subject's call to the Data User's call centre, the Data Subject did not indicate the date and approximate time of Data Subject's call); 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/Relevant Person). 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);

- seeking the consent of the third party if practical (e.g. where the third party is easily locatable); or

- determining whether or not it will be reasonable in all the circumstances to disclose the personal data without the consent of the third party; or

(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 person making 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; or

> *Examples of what amounts to "confidential commercial information" include the Data User's methodology, systems, internal policies, processes and procedures for managing its business including its formulations as to the creditworthiness of a Data Subject, its internal controls, risk management, fraud detection/prevention/investigation, information security, anti-money laundering/terrorism financing and other regulatory compliance policies, processes and procedures or disclosure of the fact that confidential negotiations are ongoing, which might be of value to a competitor of the Data User or which may compromise the Data User's controls against fraud or other criminal activities.*

(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.

1.26 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

1.27 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.

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

(i) a copy of the DAR;

(ii) a record of the verification of the identity of the Relevant Person;

(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 / Relevant Person in question.

1.29 In handling DARs for joint accounts, the joint account mandate will apply. For example if the joint account mandate requires all account holders to sign, the DAR must be issued by all the joint account holders or by their jointly appointed Relevant Person.

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 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 that is currently within the various electronic and physical systems of the Data User as provided by the Data Subject to the Data User.

2.3 Subject to 1.4 above, any expressions of opinion held by a Data User may also be the subject of a DCR.

Format Of A DCR

2.4 A DCR does not have to be in a particular format. However, there are prerequisites that a Data Subject / Relevant Person must fulfil when making a DCR:-

(i) the DCR must be in writing (as defined in Part 2);

(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 / Relevant Person;

(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 / Relevant Person's right to make a request.

If any one of these prerequisites is not fulfilled, the Data User should return the DCR to the Data Subject / Relevant Person and ask for the omitted information / copies to be resubmitted by the Data Subject / Relevant Person.

2.5 Data Users may require the use of a standardised form for a DCR to be made but are not permitted to make it mandatory that such standardised forms are to be used when making a DCR.

2.6 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 / Relevant Person on the proper manner of making a valid DCR and provide whatever assistance as may be required by the Data Subject / Relevant Person to make a DCR.

2.7 No fees are chargeable for making a DCR.

Receipt And Processing Of A DCR

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

(i) confirmation of the identity of the Data Subject /Relevant Person or the submission of relevant certified documentation to establish the Relevant Person's right to make a request on behalf of the Data Subject; and

(ii) the personal data that requires correction being clearly specified.

2.9 The Data User will apply its identity verification processes in order to verify that the DCR is from the Data Subject or from a Relevant Person. The Data User may reject the request if the Data User is not able to verify the identity of the person making the request. The Data User is required to state the reason for the rejection to the Data Subject / Relevant Person.

2.10 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 dispatch a letter to the said Data Subject / Relevant Person informing them of the delay and the required extension, subject to it not being in excess of fourteen (14) days.

2.11 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 / Relevant Person with the sought after personal data to the extent that they are able to do so, whilst informing the said Data Subject / Relevant Person of the efforts being undertaken to provide the balance of the personal data.

Refusal To Comply With A DCR

2.12 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.

2.13 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, address, and such other related information as the Commissioner may determine) in order to establish the identity of the Data Subject/ Relevant Person, or establish the Relevant Person'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; 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

Example: Where the Data Subject alleges that the monthly bill issued by Data User is wrong but internal investigations prove otherwise.

(iv) the Data User is not satisfied that the correction requested is accurate, complete, not misleading or up-to-date.

Example: Where a Data Subject seeks a change to his / her address but the Data User has grounds to believe the new address provided by the Data Subject to be an attempt in order to avoid the service of a summons on the Data Subject.

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

2.15 Where the Data User does not comply with a DCR based on any of the reasons provided in 2.13 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.

2.16 Where the DCR relates to an expression of opinion held by a Data User not involving any matters addressed in 1.4 above, it is open to the Data User to disagree that the said expression of opinion is inaccurate, incomplete, misleading or not up-to-date. However, the Data User is obligated to:

(i) make a note as to how the expression of opinion is considered by the Data Subject submitting the DCR to be inaccurate, incomplete, misleading or not up-to-date;

(ii) either annex the note to the personal data in question (e.g. annexing the note to the physical file containing the personal data of the Data Subject) or maintain the note separately;

(ii) ensure that the expression of opinion cannot be used by any person without the note being drawn to the attention of that person and being available for inspection (e.g. by inserting a system pop-up notifying the person accessing the personal data of the differing opinions regarding the personal data in question); and

(iii) attach a copy of the note to the letter to the Data Subject/Relevant Person refusing to act on the DCR.

Administrative

2.17 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.

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

(i) a copy of the DCR;

(ii) a record of the verification of the identity of the Relevant Person;

(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 / Relevant Person in question.

2.19 In handling DCRs for joint accounts, the joint account mandate will apply. For example if the joint account mandate requires all account holders to sign, the DCR must be issued by all the joint account holders or by their jointly appointed Relevant Person.

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 The Act does not define what is meant by *"unwarranted"* and *"substantial damage or distress"*. However, in most cases:

(i) *"substantial damage"* includes financial loss suffered by the Data Subject;

(ii) *"substantial distress"* includes emotional or mental pain suffered by the Data Subject; and

(iii) *"unwarranted"* means that the damage or distress suffered by the Data Subject is not justifiable.

3.3 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 than 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"*.

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

(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).

3.5 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.

3.6 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.

3.7 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 is required to cease processing 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, i.e. the settlement of 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 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.

Example: Where the Data User receives a notice withdrawing consent to process a Data Subject's personal data which does not impinge on the rights and obligations of the Data User under contract or law, the Data User ought to:

(i) commence or follow through on collection of any outstanding bills and 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.

4.4 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.

4.5 In instances where the Data User receives a notice withdrawing consent to process the Data Subject's personal data in relation to a joint account, the said notice may be issued by any of the joint account holders. Upon receipt of such a notice, the Data User has the contractual right to terminate the joint account as the Data User is no longer able to process all the joint account holders' personal data to continue the joint account relationship.

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 practices of the banking and financial sector are addressed in greater depth in Part 4 of this Code.

5.4 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.

> *Example: Where a Data Subject provides his/her consent to an agent of the Data User to refer his/her name and contact number to the said Data User to introduce its product/services to the Data Subject, this consent shall override his/her previous decision to opt-out of receiving direct marketing materials from the Data User.*

5.5 A Data User needs to comply with the Data Subject's written request not to use the Data Subject's personal data for the purposes of direct marketing within a reasonable time frame. Where there is a need for the Data User to update relevant systems and databases in order to reflect the Data Subject's instructions, Data Users are expected (in normal circumstances) to comply with the Data Subject's request within a period of up to three (3) months.

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 credit card offers and not property loans/financing), 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 financial 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 In developing and implementing policies and procedures, Data Users should take the following points into consideration:-

(i) the policies and procedures are to be communicated to employees;

(ii) relevant employees be provided with training in relation to policies and procedures, the Act, Regulations and this Code;

(iii) employees' access to Data Subjects' personal data is to be restricted in accordance with its data access control policy and procedures;

(iv) confidentiality clauses and possible sanctions against a breach are required to be built into the employment agreement or employment manual/handbook; and

(v) procedures in the event of a breach and appropriate action to be taken against an employee responsible for the breach.

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 Relevant employees of the Data User are required to receive training on the application of the policies and procedures developed, on security and fraud awareness, as well as on compliance with the Act, Regulations and this Code.

2.3 Personal data training is required to be provided to employees as and when required. The said training needs to take into consideration the latest developments in the law and any relevant standards (or updates to the same) issued by the Commissioner.

3.0 CONTROL SYSTEM

3.1 Data Users are required to have 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 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; and
(iii) the maintenance of a database of dismissed employees,

as elaborated upon below.

Access Rights

3.3 In order to mitigate data security risks, employees' access to Data Subjects' personal data is to be controlled by Data Users adhering to their existing data access control policy and procedures for its employees.

Technical and Organizational Security Measures

3.4 Data Users are required to implement technical and organizational security measures in order to prevent personal data breaches by employees when dealing with Data Subjects' personal data.

Database of Ex-Employees

3.5 Data Users may collectively organise the maintenance of a database of ex-employees that have been dismissed by Data Users for disciplinary infractions or otherwise breaching their employment terms, or where police reports remain on record against the said ex- employee, in order to ensure that the risk to Data Users and Data Subjects' personal data is minimised. Data Users may refer to such a database prior to offering employment to an applicant who will have access to the personal data of Data Subjects.

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

2.1 It is recommended that Data Users continuously monitor their compliance with this Code, the Act, policies and procedures by:-

(i) implementing an internal monitoring framework; and

(ii) conducting self-audits.

2.2 It is recommended that Data Users implement a reporting mechanism within the organization in order that its relevant officers may report on the status of implementation of the Act, Code, the implementation and enforcement of policies and procedures, and the monitoring of issues, shortcomings or of any progress made.

2.3 It is recommended that Data Users should carry out periodic self-audits at such intervals as deemed necessary in order to identify issues in relation to compliance with the Act, the Code and the Data Users procedures and policies.

2.4 On the identification of any shortcomings and weaknesses in the implementation of the compliance framework, the Data User should ensure that appropriate remedial action is taken as soon as 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 Data User Forum makes recommendations for amendments to the Commissioner based on the results of the Code review.

3.2 The 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 THE DATA USER FORUM AND COMMISSIONER

4.1 The Data User Forum is required to liaise with the Data Users at least twice every year in respect of updates to the Code and other related matters (such as amendments to the Code and personal data protection developments within the banking and financial sector).

4.2 The 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 in the banking and financial sector.

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.

Appendix 1

Financial Services Act 2013 (Act 758)
Schedule 11

PERMITTED DISCLOSURES

First column ***Purposes for or circumstances in which customer documents or information may be disclosed***	***Second column*** ***Persons to whom documents or information may be disclosed***
1. Documents or information which is permitted in writing by the customer, the executor or administrator of the customer, or in the case of a customer who is incapacitated, any other legal personal representative.	Any person permitted by the customer or, as the case may be, the executor, administrator or legal personal representative.
2. In connection with an application for a *Faraid* certificate, grant of probate, letters of administration or a distribution order under the Small Estates (Distribution) Act 1955 [*Act 98*] in respect of a deceased customer's estate.	Any person whom a financial institution in good faith believes is entitled to obtain a *Faraid* certificate, the grant of probate, letters of administration or a distribution order.
3. In a case where the customer is declared bankrupt, is being or has been wound up or dissolved in Malaysia or in any country, territory or place outside Malaysia.	All persons to whom the disclosure is necessary in connection with the bankruptcy or winding up or dissolution.
4. Any criminal proceedings or civil proceedings between a financial institution and- *(a)* its customer, his surety or guarantor relating to the customer's transaction;	All persons to whom the disclosure is necessary for the purpose of the criminal proceedings or civil proceedings.

First column *Purposes for or circumstances in which customer documents or information may be disclosed*	*Second column* *Persons to whom documents or information may be disclosed*
(b) two or more parties making adverse claims to money in a customer's account where the financial institution seeks relief by way of interpleader; or *(c)* one or more parties in respect of property in or over which some right or interest has been conferred on the financial institution.	
5. Compliance by a licensed bank or licensed investment bank which has been served a garnishee order attaching moneys in the account of a customer.	All persons to whom the disclosure is required to be made under the garnishee order.
6. Compliance with a court order made by a court not lower than a Sessions Court.	All persons to whom the disclosure is required to be made under the court order.
7. Compliance with an order or request made by an enforcement agency in Malaysia under any written law for the purposes of an investigation or prosecution of an offence under any written law.	An investigating officer authorized under the written law to investigate or any officer authorized to carry out prosecution or any court.
8. Performance of functions of the Malaysia Deposit Insurance Corporation.	Any director or officer of the Malaysia Deposit Insurance Corporation or any other person, authorized by the Malaysia Deposit Insurance Corporation to receive the documents or information.
9. Disclosure by a licensed investment bank for the purpose of performance of	Any officer of the Securities Commission, approved stock

First column ***Purposes for or circumstances in which customer documents or information may be disclosed***	***Second column*** ***Persons to whom documents or information may be disclosed***
relevant functions of- *(a)* the Securities Commission under the securities laws as defined in the Securities Commission Act 1993; *(b)* the stock exchange or derivatives exchange approved under the Capital Markets and Services Act 2007; *(c)* the clearing house approved under the Capital Markets and Services Act 2007; or *(d)* the central depository approved under the Securities Industry (Central Depositories) Act 1991 [*Act 453*].	exchange or derivatives exchange, approved clearing house under the Capital Markets and Services Act 2007 or approved central depository under the Securities Industry (Central Depositories) Act 1991 authorized to receive the documents or information.
10. Disclosure by a licensed bank or licensed investment bank for the purpose of performance of functions of an approved trade repository under the Capital Markets and Services Act 2007.	Any officer of the approved trade repository authorized to receive the documents or information.
11. Documents or information is required by the Inland Revenue Board of Malaysia under section 81 of the Income Tax Act 1967 for purposes of facilitating exchange of information pursuant to taxation arrangements or agreements having effect under section 132 or 132A of the Income Tax Act 1967.	Any officer of the Inland Revenue Board of Malaysia authorized to receive the documents or information.
12. Disclosure of credit information of a customer to a credit reporting agency registered under the Credit Reporting Agencies Act 2010 [*Act 710*] for purposes of carrying on credit reporting business as defined in the Credit Reporting Agencies	Any officer of the credit reporting agency authorized to receive the documents or information.

First column *Purposes for or circumstances in which customer documents or information may be disclosed*	*Second column* *Persons to whom documents or information may be disclosed*
Act 2010.	
13. Performance of any supervisory functions, exercise any of supervisory powers or discharge any of supervisory duties by a relevant authority outside Malaysia which exercises functions corresponding to those of the Bank under this Act.	Any officer of the relevant authority authorized to receive the documents or information.
14. Conduct of centralized functions, which include audit, risk management, finance or information technology or any other centralized function within the financial group.	The head office or holding company of a financial institution whether in or outside Malaysia or any other person designated by the head office or holding company to perform such functions.
15. Due diligence exercise approved by the board of directors of the financial institution in connection with- *(a)* merger and acquisition; *(b)* capital raising exercise; or *(c)* sale of assets or whole or part of business.	Any person participating or otherwise involved in the due diligence exercise approved by the board of the financial institution.
16. Performance of functions of the financial institution which are outsourced.	Any person engaged by the financial institution to perform the outsourced function.
17. Disclosure to a consultant or adjuster engaged by the financial institution.	Consultant or adjuster engaged by the financial institution.
18. A financial institution has reason to suspect that an offence under any written law has been, is being or may be	Any officer of another financial institution or the relevant associations of financial institutions

First column *Purposes for or circumstances in which customer documents or information may be disclosed*	*Second column* *Persons to whom documents or information may be disclosed*
committed.	authorized to receive the documents or information.