Code of Practice on Personal Data Protection for the Insurance and Takaful Industries in Malaysia

Part A - Introduction

1. Introduction

1.1. This Code of Practice ("**Code**") is issued pursuant to Section 23(1)(a) of the Personal Data Protection Act 2010 ("**Act**") in Malaysia as a collective initiative of the:

(a) Life Insurance Association of Malaysia ("**LIAM**");
(b) General Insurance Association of Malaysia ("**PIAM**"); and
(c) Malaysian Takaful Association ("**MTA**"),

(collectively referred to as the "**INSURANCE and TAKAFUL ASSOCIATIONS**").

1.2. LIAM is a trade association with its objectives to promote a progressive life insurance industry; to enhance public understanding and appreciation for life insurance; to upgrade the image and professionalism of the life insurance industry and to support the regulatory authorities in developing a strong industry.

1.3. PIAM is a trade association with its objectives to articulate one unified voice for and on behalf of the general insurance industry; to create favourable business environment for member companies, promote the image of the general insurance industry and its role in the economy; to educate consumers on general insurance products; foster public confidence by protecting the interests of consumers; to establish a sound and efficient insurance infrastructure with best practices; to raise professionalism and ensure standards in distribution; to harmonize approaches and solutions to industry issues; to build a pipeline of talent and to profile general insurance as a career of choice and to facilitate information sharing within boundaries of the Competition Act 2010 and other laws of Malaysia.

1.4. MTA is a trade association with its objectives to build a sustainable, profitable and growing Takaful industry in Malaysia; an industry that can be trusted and recognized as contributing to society and the economy; an economic and public policy climate conducive to a flourishing industry and to become a trade body recognized as providing active leadership and to act as an authoritative collective voice for the Takaful industry.

1.5. For the purposes of this Code, the following terms shall have the meaning as defined below:

"**BNM**" refers to Bank Negara Malaysia.

"**Data Processor**" refers to 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 its own purposes.

"**Data User**" refers to 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.

"**Data Subject**" refers to an individual to whom the personal data relates to, including but not limited to a proposer, a policyholder/certificate holder, an insured person/covered person, a beneficiary, a nominee, a trustee, a claimant, their authorized representative and any other individual whose personal data is being assessed, processed or negotiated pursuant to the insurance/takaful business, and collectively to be referred to as "**Data Subjects**".

"**FIS**" refers to the Fraud Intelligence System, an information-sharing system which utilizes analytical techniques for fraud prevention and detection, which is operated by Insurance Services Malaysia Berhad (or any other company engaged for the operation of the FIS from time to time).

"**FSA/IFSA**" refers to the Financial Services Act 2013/Islamic Financial Services Act2013.

"**Insurer/Operator**" refers to an insurance company/takaful operator licensed under the FSA/IFSA, and duly registered as a Data User with the Personal Data Protection Commissioner ("**Commissioner**") under the Act, and collectively to be referred to as "**Insurers/Operators**". Unless expressly stated otherwise, Insurers/Operators shall include Insurance/Takaful Intermediaries (as defined below).

"**Insurance/Takaful Intermediary**" refers to an insurance/takaful agent registered with one of the INSURANCE and TAKAFUL ASSOCIATIONS, collectively to be referred to as "**Insurance/Takaful Intermediaries**" but does not include independent insurance/takaful broker and financial adviser.

"**Joint Insurance Takaful Council**" refers to the council consisting representatives from LIAM, PIAM and MTA having the objective of promoting and protecting the interest of their respective members in connection with life insurance business, general insurance business and takaful business respectively in Malaysia.

1.6. For purposes of interpreting this Code:

(a) words importing one gender shall include all other genders, and words importing the singular shall include the plural and vice versa;

(b) references to "persons" shall include bodies corporate, unincorporated associations and partnerships (whether or not having separate legal personality);

(c) references to any person includes their/its respective personal representatives, successors and assigns; and

(d) any references, express or implied, to statutes or statutory provisions shall be construed as references to those statutes or provisions as respectively amended or re-enacted or as their application is modified from time to time by other provisions (whether before or after the date hereof) and shall include any statutes or provisions of which they are re-enactments (whether with or without modification) and any orders, regulations, instruments or other subordinate legislation under the relevant statute or statutory provision.

1.7. This Code was drafted in consultation with the Personal Data Protection Commission ("**PDP Commission**") and the INSURANCE and TAKAFUL ASSOCIATIONS.

1.8. The objective of this Code is to set out best practices for Insurers/Operators to assist them in meeting the requirements under the Act when undertaking insurance/takaful businesses and activities. This Code sets out the seven (7) personal data protection principles ("**PDP Principles**") of the Act.

1.9. Every Insurer/Operator is required to have due regard to this Code in the course and operation of their insurance/takaful business, particularly in handling and management of personal data of their Data Subjects in Malaysia.

1.10. This Code must be read together with any guidelines, directives and codes of practice issued by the PDP Commission, the INSURANCE and TAKAFUL ASSOCIATIONS as well as other relevant regulatory authority such as BNM from time to time, particularly those which are relevant or applicable to the insurance/takaful industry in Malaysia. This Code may therefore be amended, revised or updated, as required, to include any changes in the applicable laws, guidelines, directives or codes of practice from time to time and to the type of personal data collected and processed by the insurance/takaful industry.

1.11. All words, phrases or terms used in this Code shall have the same meaning as defined under the Act, the FSA/IFSA and any rules, regulations, standards, guidelines, codes of practice and circulars issued thereunder, unless defined or stated otherwise in this Code.

2. Acceptance of the Code by the Commissioner

2.1. This Code applies to the processing of personal data including sensitive personal data of a Data Subject, by all Insurers/Operators in the insurance/takaful industry in Malaysia.

2.2. This Code has been accepted by the Commissioner pursuant to Section 23(4) of the Act, wherein:

(a) the Code is consistent with the provisions of the Act;

(b) the purpose for the processing of personal data by the Insurers/Operators has been taken into consideration;

(c) the views of the Data Subjects whose personal data are processed by an Insurer/Operator or groups representing such Data Subjects have been taken into consideration;

(d) the views of the regulator of the insurance/takaful sector (i.e. BNM) have been taken into consideration; and

(e) the Code offers an adequate level of protection for the personal data of the Data Subjects concerned.

2.3. This Code has been drafted in the English language. In case of discrepancies between the English text version of this Code and the Bahasa Malaysia version (or any other translated version), the English version shall prevail.

3. Effective Date

3.1. Pursuant to Section 23(4) of the Act, this Code shall be effective from the date of registration of the Code by the Commissioner in the Register of Codes of Practice ("**Effective Date**").

3.2. Where an Insurer/Operator has processed personal data of the Data Subject before the Effective Date, it will be deemed to have complied with this Code so long as the processing activities are not inconsistent with the Act.

4. Legal Force and Effect of the Code

4.1. All Insurers/Operators dealing with personal data are bound to comply with this Code by virtue of Section 25 of the Act.

4.2. An Insurer/Operator that fails to comply with any mandatory provision of this Code will be deemed to have committed an offence and, upon conviction, the non-compliant Insurer/Operator will be liable to a fine of up to one hundred thousand ringgit (RM100,000) or an imprisonment term of up to one year or both, as stipulated in Section 29 of the Act.

4.3. Compliance with this Code shall be a defence against any action, prosecution or proceeding of any nature, brought against an Insurer/Operator, whether in court or otherwise, for one or more alleged breaches of the Act and/or regulations under the Act.

4.4. In respect of the Insurance/Takaful Intermediaries, to the extent where the Insurance/Takaful Intermediaries are in a position to comply, the Insurers/Operators shall, in the interest of upholding the professional standard of Insurance/Takaful Intermediaries in Malaysia and for the protection of consumers, require the Insurance/Takaful Intermediaries to comply with all the relevant obligations under this Code.

5. Personal Data Processing Operations in Insurance/Takaful Industry

5.1. The processing operations which are relevant to the insurance/takaful industry include but not limited to the following:

(a) handling applications to purchase insurance policies/participate in takaful certificates and/or requests for advice and product recommendations;
(b) preparing, issuing and handling other administrative matters relating to the insurance policies/takaful certificates;
(c) collecting premiums/contributions and submitting other bills;
(d) processing and settling claims and paying other benefits;
(e) regular assessment after purchase of insurance/participation in takaful products;
(f) re-insurance/re-takaful;
(g) co-insurance/co-takaful;
(h) preventing, detecting, investigating and/or prosecuting actual or suspected insurance/takaful fraud and other criminal activities;
(i) establishing, exercising or defending a legal claim;
(j) meeting other specific legal or contractual obligation;
(k) prospecting new insurance/takaful markets, including research for product and service development;
(l) internal management;

(m) disclosure to third parties as provided for under the Disclosure Principle in this Code and the Act;
(n) audit, risk assessment, survey, statistical and analytical studies relating to the insurance/takaful business;
(o) discharging regulatory or legislative obligations; and/or
(p) actuarial activities.

5.2. For the purposes of the processing operations as set out in the foregoing, Insurers/Operators will likely collect and obtain the following personal data of the Data Subjects:

Non-Sensitive Personal Data:

(a) name and age;
(b) home/mailing address;
(c) NRIC/passport number;
(d) contact information, telephone number, email address;
(e) biodata/personal profile;
(f) photograph or video image of an individual;
(g) employment information;
(h) financial information;
(i) investment and risk preferences in respect of investment type products;
(j) vehicle registration numbers;
(k) personal data of family members/next-of-kin;
(l) personal data of the beneficiaries or nominees relevant to the processing of insurance/takaful claims, the provision of the insurance/takaful and related products and services; and/or
(m) such other personal data required with Data Subject's consent.

Sensitive Personal Data:

(a) thumbprint or DNA profile;
(b) physical and/or mental health condition;
(c) religious belief;
(d) commission or alleged commission of any offence or contravention of any laws at any point of time;
(e) expression of opinion; and/or
(f) such other sensitive personal data required with Data Subject's consent.

5.3. It is mandatory for a Data Subject to supply both the non-sensitive and sensitive personal data requested by the Insurers/Operators. The Insurers/Operators will inform the Data Subject when the supply of certain personal data by the Data Subject is optional or mandatory for the purposes of taking out an insurance policy/takaful certificate.

5.4. For the purposes of this Code, the term "**personal data**" is as defined in the Act, and shall include "**sensitive personal data**" as defined in the Act, namely, a Data Subject's physical or mental health or condition, religious belief, commission or alleged commission of any offence or contravention of any laws at any point of time as well as expression of opinion about a Data Subject which are likely to arise during the course of processing the Data Subject's personal data.

5.5. In the course of dealings with Data Subjects, all Insurers/Operators must comply with all seven (7) Personal Data Protection Principles below:

(a) General Principle;
(b) Notice and Choice Principle;
(c) Disclosure Principle;
(d) Security Principle;
(e) Retention Principle;
(f) Data Integrity Principle; and
(g) Access Principle,

unless their personal data processing activities fall under one of the exceptions of the Act.

Part B – Data Subject's Rights

6. Subject to the exemptions and exceptions stated in any laws, rules, regulations, this Code and the Act, a Data Subject has the following rights, namely:

6.1. Right of access to personal data - a Data Subject is entitled to be informed by an Insurer/Operator whether his personal data is being processed by or on behalf of the Insurer/Operator.

6.2. Right to correct personal data - a Data Subject is entitled to correct his personal data if it is inaccurate, incomplete, misleading or not up-to-date.

6.3. Right to withdraw consent - a Data Subject is entitled to withdraw his consent to the processing of personal data.

6.4. Right to prevent processing likely to cause damage or distress - a Data Subject is entitled to request the Insurer/Operator to cease or not begin the processing of his personal data based on the reasons that the processing of that personal data is causing or likely to cause substantial damage or substantial distress to him or to another; and the damage or distress is or would be unwarranted.

6.5. Right to prevent processing for purposes of direct marketing - a Data Subject is entitled to request the Insurer/Operator to cease or not begin processing his personal data for purposes of direct marketing.

Part C – Personal Data Protection Principles

7. General Principle

7.1. Insurers/Operators collect personal data through various modes of communication including proposal forms, claim forms and other documentation completed or provided by the Data Subjects, as well as verbally e.g. via face-to-face, phone calls or electronically, e.g. by point of sale systems or over the Internet.

7.2. The collection and processing of personal data by Insurers/Operators usually happens at various main stages, such as:

(a) pre-contractual stage, including advising, marketing, application or proposal stage;
(b) contractual stage, during the term of the insurance policy/takaful certificate; and
(c) claim stage.

7.3. As a general rule, Insurers/Operators will be allowed to process the Data Subjects' personal data in accordance with the provisions of the Act and, if required, where consent has been obtained from the relevant Data Subjects.

7.4. Where processing of personal data is necessary to:

(a) enable an Insurer/Operator to conduct its insurance/takaful business, including but not limited to the processing for the purposes described in Paragraph 8.6 below;
(b) carry out the instructions of a Data Subject, including but not limited to updating the insurance policy/takaful certificate, updating personal data, appointment of Insurance/Takaful Intermediaries, enquiring about premium payment status of an insurance policy/takaful certificate; and/or
(c) confer an interest or a benefit on a Data Subject under a life insurance, general insurance, family takaful, general takaful, medical insurance/takaful, group insurance policies or group takaful certificates,

the relevant Data Subject concerned will be deemed to have given his consent (including explicit consent) to the collection, use, disclosure and processing of his personal data by the Insurer/Operator as required under Section 6(1) and Section 40 of the Act if he voluntarily provides his personal data to the Insurer/Operator for any of the purposes above, and it is reasonable that he would do so.

7.5. Paragraph 7.4 above does not prevent an Insurer/Operator from getting express written consent from a Data Subject in any event.

7.6. Paragraph 8 sets out other circumstances in which a Data Subject is deemed to have given his consent.

7.7. <u>Processing of personal data relating to third party individuals</u>

7.7.1. Data Subject may give or may be deemed to have given consent for disclosure of his personal data by an Insurer/Operator and/or the INSURANCE and TAKAFUL ASSOCIATIONS to another organisation for any of the purposes set out in Paragraphs 8.5 and 8.6 below and to any categories of persons set out in Paragraph 9.2 below.

7.7.2. Where a proposer provides personal data of any third party to the Insurer/Operator (e.g. in respect of a group insurance policy/group takaful certificate, or a policy/certificate taken on the life of another person), or where he names a third party as life assured, beneficiary, nominee, trustee, assignee, and personal data is not collected directly from the third party individual himself, consent is deemed to have been given to the proposer to process and disclose the third party individual's personal data to the Insurer/Operator. The said third party shall be deemed to have given his consent (including explicit consent) to the collection, use and disclosure of his personal data by the Insurer/Operator as required under Section 6(1) and Section 40 of the Act to any categories of persons set out in Paragraph 9.2 below for the insurance/takaful application and processing purposes, to carry out the instructions of the proposer, and/or to confer an interest or a benefit on the third party under a life insurance, general insurance, family takaful, general takaful, medical insurance/takaful, group insurance policies or group takaful certificates.

7.7.3. In the case of an independent insurance/takaful broker or financial adviser who acts on behalf of the proposer, consent is deemed to have been given to the independent insurance/takaful broker or financial adviser to process and disclose the proposer's personal data to the Insurer/Operator. The proposer shall be deemed to have given his consent (including explicit consent) to the collection, use and disclosure of his personal data by the Insurer/Operator as required under Section 6(1) and Section 40 of the Act to any categories of persons set out in Paragraph 9.2 below for the purpose of providing the proposer with the insurance/takaful services requested by him, to carry out the instructions of the proposer, and/or to confer an interest or a benefit on the proposer under a life insurance, general insurance, family takaful, general takaful, medical insurance/takaful, group insurance policies or group takaful certificates.

7.7.4. In the case of an independent party who is involved in an insurance/takaful claim for a Data Subject, such as claim investigation company, loss adjuster/surveyor, police, hospital, law firm, workshop, vehicle towing company, etc, consent is deemed to have been given to these independent parties to process and disclose the Data Subject's personal data to the Insurer/Operator. The Data Subject shall be deemed to have given his consent (including explicit consent) to the collection, use and disclosure of his personal data by the Insurer/Operator as required under Section 6(1) and Section 40 of the Act for the purpose of processing his insurance/takaful claim and disclosing his personal data to to any categories of persons set out in Paragraph 9.2 below.

7.8. Minor or person who is incapable of giving consent

(a) As a general rule, if the Data Subject is under the age of 18 years, the Insurer/Operator must obtain the consent from his parent, guardian or person who has parental responsibility for that Data Subject.

(b) Notwithstanding Paragraph 7.8(a), if the Data Subject has attained the age of 16 years **AND** he wishes to effect a life policy/ participate in a family takaful certificate on his own life or on another life in which he has an insurable interest/ permissible takaful interest, he is deemed to have the capacity to give consent on his own, and no consent is required from his parent, guardian or person who has parental responsibility over him in respect of his personal data in relation to that life policy/takaful certificate.

(c) If the Data Subject is incapable of managing his own affairs, for example due to physical or mental incapacity, the Insurer/Operator must obtain the consent from a person who is appointed by a court to manage the affairs of the Data Subject or a person authorised in writing by the Data Subject to act on his behalf.

7.9. Withdrawal of consent

(a) Unless it prevents any of the relevant Insurer/Operator from performing its obligations to any Data Subject or goes against the very purpose that the personal data was given as provided in this Code, the relevant Data Subject may withdraw consent by letting the relevant Insurer/Operator know in writing in the manner and format as may be prescribed by each of the relevant Insurer/Operator. In such instances, the Insurer/Operator will inform the Data Subject of the consequences of such withdrawal of consent, including termination of the insurance/takaful contract

or policy, or that the Insurer/Operator would be unable to continue providing services to the Data Subject. The Data Subject will have to bear all legal consequences arising from such withdrawal of consent and subsequent termination of the insurance policy/takaful certificate.

(b) Upon withdrawal of consent, the Insurer/Operator is required to, within a reasonable time frame, cease collecting, using or disclosing the Data Subject's personal data.

(c) Notwithstanding withdrawal of consent, the Insurer/Operator and any information-sharing systems for fraud prevention and detection, including but not limited to the FIS, may still retain the Data Subject's personal data that is required for operational, audit, investigation, legal, regulatory, tax or accounting requirements, for example, keeping records of the Data Subject's product purchases/participation which are reasonably necessary for audit purposes, processing the personal data pertaining to an insurance/takaful claim, complying with the various legal or regulatory requirements for keeping books of accounts or customers' records, the handling of potential litigation and future possible cases of underwriting and claims assessment, or for the purposes described in Paragraph 9.5 below. Such right shall not be prejudiced nor affected by the withdrawal of consent by the Data Subject.

8. Notice and Choice Principle

8.1. All Insurers/Operators (excluding Insurance/Takaful Intermediaries) are required to post an adequate privacy notice/policy ("**Privacy Notice/Policy**") on their website or via any other form of communication or public notice for the information of their new and existing Data Subjects and allowing the Data Subject to contact the relevant Insurer/Operator in the event the said Data Subject has any complaints, objections or inquiries in respect of his personal data.

8.2. The Privacy Notice/Policy must contain the necessary information as set out under Section 7(1) of the Act.

8.3. For all personal data that an Insurer/Operator holds prior to the Effective Date, unless the Data Subject requests for a written copy of the Privacy Notice/Policy, the posting of the Privacy Notice/Policy on the Insurer's/Operator's website or via any other form of communication or public notice, as the Insurer/Operator deems appropriate, will fulfill the Notice and Choice Principle's requirement of a written notice under Section 7 of the Act; whereas for all new personal data collected from the Effective Date onwards, the Data Subject must be given a written copy (whether by hardcopy or by e-mail) of the Privacy Notice/Policy, unless the personal data was collected via website (for example, queries or feedback by Data Subject on website, or other social media platforms) and reference has been made to the Privacy Notice/Policy in the Insurer/Operator's website.

8.4. A valid deemed consent would arise when the Data Subject is informed, made aware of, or knew the purpose for which his personal data would be processed, which are as set out under Paragraphs 8.5 and 8.6 below, and the Data Subject provides his personal data for this purpose or the personal data is furnished for the benefit of third party individuals.

8.5. For each of the INSURANCE and TAKAFUL ASSOCIATIONS, the purposes of processing of personal data shall include the following:

(a) information sharing for the upholding of professional standard of Insurance/Takaful Intermediaries in Malaysia and for the protection of consumers by preventing the appointment of unethical Insurance/Takaful Intermediaries, or Insurance/Takaful Intermediaries who have committed acts of misconduct or fraud, or have engaged in unethical practices, in the insurance/takaful industry, as registered with each of the INSURANCE and TAKAFUL ASSOCIATIONS, including the sharing of this information between the INSURANCE and TAKAFUL ASSOCIATIONS as agreed by the Joint Insurance Takaful Council;

(b) the identification, prevention, deterrence and investigation of any actual or suspected insurance/takaful fraud or conspiracy claim against Insurers/Operators or which may cause a fiscal threat to the insurance/takaful industry for the protection of consumers;

(c) the compliance with any guidelines, circulars or directives issued by the PDP Commission, BNM or any other applicable authorities; and

(d) cooperating with the PDP Commission, BNM or any other applicable authorities to conduct an audit, examination or investigation which is authorised under any applicable Malaysian laws.

8.6. For Insurers/Operators, in addition to Paragraph 8.5 above, the purposes of processing of personal data shall also include the following:

(a) the conduct of insurance/takaful business, i.e. carrying out any activity in relation to or in connection with carrying out duties as an Insurer/Operator, as licensed under the FSA/IFSA;

(b) the performance of obligations including customer service under a written agreement, complaints handling, conservation, including any value-added services that are connected but not directly connected to such agreement, where such agreement shall include but not be limited to life insurance, general insurance, family takaful, general takaful, medical insurance/takaful, group insurance policies or group takaful certificates, agency contract, broking arrangements, and employment contract;

(c) investigation during underwriting and claims assessment or at any time during the concurrence of the insurance policy/takaful certificate that is necessary and reasonable to identify any possible non-disclosure of material information in an insurance/takaful fraud or conspiracy claim, including but not limited to the purposes of medical/health/life insurance, requesting and verifying information with any medical practitioner, hospital, medical institution or any person (whether incorporated or not) who has ever attended to the Data Subject or has records on the health of the Data Subject; the purposes of motor insurance, requesting and verifying information with any motor companies, workshops, or any person (whether incorporated or not) who has ever attended to the Data Subject or has records on the motor vehicles belonging to the Data Subject; and the Insurer/Operator and/or its relevant Data Processors may keep such records for future possible cases of underwriting and claims assessment;

(d) exercising the right of subrogation/recovery;

(e) for the purposes of preventing, investigating, reporting or otherwise in relation to actual or suspected money laundering, terrorist financing, bribery, corruption, actual or suspected fraud including but not limited to insurance/takaful fraud, tax evasion, evasion of economic or trade sanctions, and criminal activities generally or other unlawful activities;

(f) compliance with the requirements of any law, any regulations or guidelines, any present or future contractual or other commitment with any legal, regulatory, judicial, administrative, public or law enforcement body, whether in or outside Malaysia, that are issued by regulatory or other authorities with which the Insurer/Operator or any other group members of the Insurer/Operator need or are expected to comply, including but not limited to making any enquiries, any investigation, disclosure or reporting requirements and/or meeting obligations pursuant to such law, regulations guidelines and/or the relevant authorities;

(g) cooperating with the PDP Commission, BNM or any other relevant authority to conduct an audit, examination or investigation which is authorised under any applicable Malaysian laws or international treaties/agreements affecting Insurers/Operators, whether directly or through the group of companies to which such Insurers/Operators belong;

(h) marketing (including direct marketing) to any Data Subject of insurance or takaful products, provided that such Data Subject has not given written instructions pursuant to Section 43 of the Act to cease processing his personal data for direct marketing purpose;

(i) matching personal data held in relation to a Data Subject for any purposes contained in this paragraph, specifically but not limited to those as set out at sub-paragraphs (e), (f), and (g) above;

(j) research, audit purposes and risk assessment/survey, including statistical/actuarial research or data analytics/study. In the event such data was required for this purpose, the Data Subjects' personal data are not to be published, and only figures, statistics and general information in the findings of the study/research are to be published;

(k) the performance of obligations under any lawful scheme of transfer of business;

(l) cooperating or assisting in investigations undertaken by another Insurer/Operator or any of the INSURANCE and TAKAFUL ASSOCIATIONS;

(m) conducting investigation on any Insurance/Takaful Intermediaries and their third party service providers for any allegation of fraud, conspiracy, breach of any laws, rules and regulations, codes of practice including this Code, misconduct or any unethical behaviours or practices;

(n) performing re-insurance/re-takaful;

(o) information sharing with the INSURANCE and TAKAFUL ASSOCIATIONS and any information-sharing systems; and/or

(p) all the other processing operations mentioned in Paragraph 5.1 above.

8.7. Any personal data requested, collected, obtained, stored, retained and/or otherwise processed from time to time by any of the INSURANCE and TAKAFUL ASSOCIATIONS and/or Insurers/Operators that are directly related to the purposes described at Paragraphs 8.5 and 8.6 above are deemed necessary for the purposes of this Code, and consent (including explicit consent) would be deemed to have been given by the Data Subjects.

8.8. All personal data requested by each of the Insurers/Operators from the Data Subjects to supply for the purposes described at Paragraph 8.6 above (save for Paragraph 8.6(h)) are obligatory unless stated otherwise. The consequences for failing to supply the requested personal data to Insurers/Operators may include the Insurers/Operators being unable to perform its obligations to the Data Subjects.

8.9. While the Act allows a Data Subject to withdraw his consent for the processing of his personal data, any withdrawal of consent by the Data Subject for any of the purposes described at Paragraph 8.6 above (save for Paragraph 8.6(h)) may result in the termination of the insurance policy/takaful certificate that the Data Subject currently has with the Insurer/Operator, and the Data Subject will have to bear all legal consequences arising from such withdrawal of consent and subsequent termination of the insurance policy/takaful certificate. The Insurer/Operator must inform the Data Subject of the likely consequences of withdrawing consent when it receives the Data Subject's notice of withdrawal of consent.

9. Disclosure Principle

9.1. An Insurer/Operator may only disclose the Data Subject's personal data for the purposes for which the personal data is being, or is to be collected and further processed. This means that personal data must not be collected for one purpose and then used for a different purpose.

9.2. Further, subject to notification within the respective Insurer's/Operator's Privacy Notice or as otherwise permitted under the Act, an Insurer/Operator may disclose the Data Subject's personal data to the following third parties:

(a) individuals or organizations within the relevant Insurer's/Operator's Group of Companies, or another Insurer's/Operator's Group of Companies, strictly on a need to know basis;

(b) bancassurance partners, third party outsourcing service providers, third party call centres, Insurance/Takaful Intermediaries, independent insurance/takaful broker or financial adviser;

(c) re-insurers/re-takaful service providers or retrocessionaires;

(d) claims investigation companies or loss adjusters/surveyors or other parties necessary to process the personal data for claims purposes;

(e) relevant government authorities, law enforcement agencies, courts, tribunals, regulatory bodies and/or statutory agencies or bodies or any other person the

Insurer/Operator is under an obligation or required or expected to make disclosures for the purposes set out, or in connection with Paragraphs 8.6(e), (f) or (g);

(f) industry associations and federations;

(g) doctors, medical specialists, hospitals, clinics or healthcare institutions;

(h) Insurer's/Operator's auditors, consultants, lawyers, accountants, fund managers or other professional advisers appointed in connection with the Insurer's/Operator's business on a strictly confidential basis, appointed to provide services to the Insurer/Operator;

(i) banks, credit card companies or other financial institutions for purposes of collection or refund of any monies due or payable;

(j) any person permitted by the Data Subject or, as the case may be, the executor, administrator or legal personal representative of the Data Subject;

(k) information-sharing systems, for purposes of enabling exchange of information between the Insurers/Operators in order to facilitate fraud prevention and detection;

(l) any person to whom disclosure is necessary for the purpose of investigation into any allegation of Insurance/Takaful Intermediaries' and their third party service providers' breach of any laws, rules and regulations, codes of practice including this Code, misconduct or unethical behaviours or practices;

(m) any person to whom the disclosure is necessary for the purposes of investigations under any written law, criminal proceedings or civil proceedings, or any person to whom the disclosure is required to be made under court order; and/or

(n) other third party service providers appointed to provide administrative, telecommunications, payment, data processing, data storage, or other services to the relevant Insurer/Operator and/or to any member of the Insurer's/Operator's Group of Companies and/or the INSURANCE and TAKAFUL ASSOCIATIONS in connection with the purposes described in Paragraphs 8.5 and 8.6 above.

For the purpose of this Paragraph 9.2, "Insurer's/Operator's Group of Companies" means the parent/holding companies of the Insurer/Operator, as well as the subsidiaries of both the parent/holding companies and the Insurer/Operator.

9.3. An Insurer/Operator must maintain an internal record of the categories of third parties to which the personal data of a Data Subject has been disclosed by the Insurer/Operator and for what purposes. This is so that the Insurer/Operator can track and monitor how and to whom the personal data in the Insurer's/Operator's possession has been disclosed to.

9.4. Where such organizations or third parties as set out in Paragraph 9.2 above are not located in Malaysia, the relevant Insurer/Operator may transfer the relevant personal data to places outside of Malaysia in accordance with Section 129 of the Act.

9.5. The disclosure of personal data (including all personal data relating to the applications/proposals for insurance (including but not limited to any upgrades), policies, claims) by an Insurer/Operator to any of the INSURANCE and TAKAFUL

ASSOCIATIONS, other Insurers/Operators and/or any information-sharing systems for the prevention or detection of crime or for the purpose of investigations, the apprehension of offenders or institution of legal proceedings shall be exempted under Section 45(2)(a) of the Act, which shall include but are not limited to the following circumstances:

(i) Insurance/Takaful Intermediaries who have committed acts of breach, misconduct or fraud, or have engaged in unethical behaviours or practices, in the insurance/takaful industry, in accordance with the prevailing rules, regulations or guidelines of the relevant INSURANCE and TAKAFUL ASSOCIATION;

(ii) sub-standard hospitalisation and disabilities cases;

(iii) life, general or family/general takaful policy/certificate proposals by sum insured/assured and type of plans for early detection of possible fraud; and

(iv) past and/or current claims information and personal data for the purposes of underwriting evaluation, analysis, investigation and fraud detection.

The personal data referred to in this Paragraph 9.5 shall include the personal data of:

(i) Data Subjects who are policyholders/certificate holders, and their authorized representatives;

(ii) lives assured, beneficiaries, nominees, trustees and/or assignees under an insurance/takaful cover;

(iii) past and/or current Insurance/Takaful Intermediaries of the Insurers/Operators including their third party service providers;

(iv) Data Subjects who apply for insurance/takaful cover and are subsequently rejected or declined for cover by the Insurers/Operators;

(v) third party insurance/takaful claimants and their authorized representatives;

(vi) Data Subjects who apply for insurance/takaful cover and who subsequently withdraw their insurance/takaful applications for cover from the Insurers/Operators; and/or

(vii) any other relevant Data Subjects who have/are suspected of committing acts of crime, misconduct or fraud.

10. Security Principle

10.1. As the contents in Paragraph 10.2 below are meant to be used as a guide for Insurers/Operators, each Insurer/Operator shall be at liberty to determine its own security measures, so long as the Insurer/Operator develops and implements a security policy that complies with the Security Principle requirements under the Act and with any regulations and guidelines as issued by BNM and the PDP Commission from time to time in relation to the security standards.

10.2. To comply with the Security Principle, Insurers/Operators will need to ensure that they take practicable security measures to prevent unauthorised access to, or alteration,

disclosure or destruction of the personal data and prevent their accidental loss, destruction, access or other similar risks. In particular, Insurers/Operators will need to establish internal policies, processes and procedures by taking into consideration and being guided by the following standards and best practices. All of the following are not meant to be prescriptive or exhaustive, and shall be referred to by the Insurers/Operators as a guiding principle in determining the level and type of security that is necessary to protect personal data:

10.2.1. Security Policy

Insurers/Operators to develop and implement a security policy, and in doing so to consider whether there is a need to give emphasis on the following management and organizational measures:

(i) enabling co-ordination systems among key personnel in the organisation (for example, the security manager will need to know about commissioning and disposing of any IT equipment);

(ii) access to premises or equipment given to anyone outside the organisation (for example, for computer maintenance) and the additional security consideration this will generate;

(iii) business continuity arrangements that identify how to protect and recover any personal data the organisation holds; and

(iv) periodic checks to ensure that the organisation's security measures remain appropriate and up to date.

10.2.2. Personal Data Security Management

The nature of security standards will vary depending on the nature of the personal data, where sensitive personal data is to be afforded a higher level of protection, the amount, distribution, format and method of storage of the different types of personal data and shall take into account the following requirements and other best practices:

(i) physical protection such as designing access area or lock-up system;

(ii) awareness among employees on the security policies and standards of the personal data of the organization;

(iii) organizational safeguards such as information and communications technology (ICT) security training, security clearances or access control; and

(iv) technology measures such as password or encryption or biometric techniques.

10.2.3. Risk Management

The Act requires that practical steps be taken to safeguard the processing of personal data since there is no one particular security solution that fits the risks of the Insurer's/Operator's establishment. In evaluating the appropriate security requirements to protect personal data, the Insurer/Operator shall consider whether there is a need for the following aspects to be taken into consideration:

(i) the nature and extent of the Insurer's/Operator's premises and computer systems used;

(ii) number of employees;

(iii) access systems to the personal data by employees; and

(iv) personal data held or used by a third party on behalf of the Insurer/Operator.

10.2.4. Access Control

The requirements of the Act go beyond the way personal data is stored or transmitted and thus the Insurer/Operator shall consider whether there is a need for the following personal data access control measures to be adopted:

(i) only authorized employees can access, alter, disclose or destroy personal data;

(ii) the relevant employees can only act within the scope of their authority; and

(iii) establishing monitoring systems to track and recover lost, altered and destroyed personal data.

10.2.5. Protection Level

The Insurer/Operator shall consider whether there is a need to set up a security level that takes into account the following aspects:

(i) the nature of personal data; and

(ii) the harm that might result from its improper use, accidental loss or destruction.

10.2.6. Staff Responsibility

The Insurer's/Operator's employees and Insurance/Takaful Intermediaries must be made to understand and to be aware of the importance of protecting personal data including their security policy. The Insurer/Operator shall determine whether initial and refresher trainings are necessary, and if so, the method and content of the training by including the following areas:

(i) duties of the Insurer/Operator under the Act and restrictions on the use of personal data;

(ii) legal implication of the Insurer's/Operator's employees and Insurance/Takaful Intermediaries who deliberately try to give access, alter or disclose personal data without authority;

(iii) proper procedures to use to identify and authenticate the identity of individual requesting for access to, or correction of, his personal data; and

(iv) any restriction imposed by the Insurer/Operator on their employees with regard to personal use of office computers and equipment to prevent virus infection or spam etc.

10.2.7. Physical security

The Insurer/Operator shall put in place key physical measures to protect personal data, such as limiting access to premises, ensuring minimum standards and quality of doors and locks, installing alarms, and closed-circuit television (CCTV) on the premises.

In addition, an Insurer/Operator must ensure that physical files are kept secure all the time and electronic files are backed-up regularly.

10.2.8. Computer security

The Insurer/Operator shall consider the computer security requirements to be put in place by taking into account the following:

(i) computer security needs to be appropriate to the size and use by the Insurer's/Operator's organization's system;

(ii) appropriate technological development that should be taken into account; and

(iii) appropriate security measures must be incorporated into the Insurer's/Operator's business practices.

10.2.9. Disaster management plan

Besides preventive measures, the Insurers/Operators shall also consider whether there is a need to establish a disaster management plan, and if required, whether such plan should take into account the following best practices so as to enable them to respond and manage the incident:

(i) containment and recovery including procedures for damage limitation;

(ii) assessing the risks with the breach in particular the potential adverse consequences for Data Subjects;

(iii) depending on the severity of the breach, whether it would be necessary to give notification of breaches by informing appropriate authorities including the PDP Commission, BNM, police, banks, media etc.

10.3. Where an Insurer/Operator engages a Data Processor, personal data held by the Insurer/Operator may be required to be disclosed by the Insurer/Operator to the Data Processor for the Data Processor to carry out its services. The Insurer/Operator must obtain sufficient guarantees from the Data Processor in respect of the security measures governing the processing of such personal data and ensure that the Data Processor takes reasonable steps to comply with these security measures. This can be achieved by, amongst others, imposing contractual obligations on the Data Processor and/or undertaking regular audits and/or relying on third party audit reports performed by licensed auditors on the Data Processor to ensure compliance.

11. Retention Principle

11.1. Insurers/Operators must not retain personal data for longer than is necessary for the fulfilment of the purpose for which it was collected unless such retention is necessary for their operational, audit, legal, regulatory, tax or accounting requirements.

11.2. Insurers/Operators must also take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was collected unless such retention is necessary for their operational, audit, legal, regulatory, tax or accounting requirements.

11.3. Compliance costs and security risks can be reduced if Insurers/Operators only collect and retain personal data that is necessary for their operational, audit, legal, regulatory, tax or accounting requirements and delete or anonymise personal data when it is no longer necessary in accordance with the following standards and best practices:

(a) Retention Standards

The retention period of personal data varies according to the nature of commercial transactions and other statutes and practices that govern the operational aspects of the insurance/takaful industry, such as the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001, the FSA/IFSA, the Limitation Act 1953, the Companies Act 1965, the Goods and Services Tax Act 2014, Income Tax Act 1967 as well as any other applicable guidelines and directives issued by the PDP Commission, the INSURANCE and TAKAFUL ASSOCIATIONS and other regulatory authorities such as BNM from time to time. Hence, the Insurers/Operators should consider establishing the length of time and reason for the retention of personal data. Personal data must be deleted from the computer system if there is no longer a need for the personal data to be kept.

(b) Retention Policy

The following are meant to be used as a guide for Insurers/Operators when it comes to considering whether to come up with a Retention Policy and the contents of the Retention Policy, so long as the Insurers/Operators comply with the Retention Principle requirements under the Act and with any regulations and guidelines issued by BNM and the PDP Commission from time to time in relation to the retention standards:

(i) period of retention/ retention schedule;

(ii) disposal processes;

(iii) filing system; and

(iv) accountable person/department.

(c) Retention Period

Save and except as set out in sub-paragraph (d) below, fresh consent must be obtained from the Data Subjects if personal data needs to be retained but not used after the period of time needed to fulfill the purposes for which it was collected including for

any operational, audit, legal, regulatory, tax or accounting requirements, or after the period of time where there is no longer a need for the personal data to be kept.

(d) Exemption

Personal data can be retained for a longer period of time if such retention is necessary for the following purposes:

(i) legal proceedings or a regulatory or similar investigation or obligation to produce the said information;

(ii) a crime or misconduct is suspected or detected;

(iii) information is relevant to a company in liquidation or receivership, where a debt is due to the Insurers/Operators; or

(iv) information is considered to be of potential historical importance including but not limited to the purposes described in Paragraph 7.9(c) above.

(e) The Insurers/Operators must inform the Commissioner of their self-regulated procedures of retaining and maintaining personal data, upon request by the Commissioner.

(f) Retention Schedule

The following are meant to be used as a guide for Insurers/Operators when it comes to considering whether to come up with a Retention Schedule and the contents of the Retention Schedule, so long as the Insurers/Operators comply with the Retention Principle requirements under the Act and with any regulations and guidelines issued by BNM and the PDP Commission from time to time in relation to the retention standards:

(i) description of personal data (name, address, etc.);
(ii) recommended retention period;
(iii) format (word, spread sheet etc.);
(iv) location of storage (in house or warehouse etc.); and
(v) reasons (for longer retention).

(g) Security and Disposal

All personal data must be both protected and disposed of in a manner that does not breach the Security Principle under the Act.

11.4. Insurers/Operators must use commercially reasonable endeavours to destroy or anonymise documents containing personal data as soon as the purpose for which the data was collected, or the Insurer's/Operator's purpose for keeping the personal data, is no longer being served by its retention and/or where the retention is beyond the minimum retention period(s) as prescribed by applicable Malaysian laws.

12. Data Integrity Principle

12.1. Insurers/Operators are required to take reasonable steps to ensure that the personal data collected is accurate, complete, not misleading and kept up-to-date by having regard to the purpose for which the personal data was collected. Insurers/Operators are expected to adhere to the following standards and best practices:

(a) Data Integrity Standards

Insurers/Operators must take the necessary measures to ensure that the personal data under their control are sufficiently accurate, complete and up-to-date unless limits to the requirement for accuracy are clearly set out.

(b) Procedures

Insurers/Operators are required to take reasonable steps to ensure that personal data that they keep are accurate, complete, and up-to-date by implementing appropriate procedures for the recording, correcting and disclosing personal data.

13. Access Principle

13.1. As a general rule, Data Subjects have the right of access to their personal data and the right to correct it if it is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is permitted to be refused under the Act or this Code.

13.2. Procedures or mechanisms must be put in place to allow Data Subjects to have access to their personal data. Insurers/Operators will need to respond appropriately to such requests from the Data Subjects within 21 days from any such request or such longer time as allowed for under the Act.

13.3. Data Subjects have the right to request details of their personal data that is being processed by or on behalf of the Insurers/Operators and to have a copy of such personal data communicated to them ("**Personal Data Access Request**"). The Insurers/Operators may charge fees prescribed/regulated by the Act for such Personal Data Access Request from the Data Subjects.

13.4. Insurers/Operators are allowed to take into account any amendment or deletion made to the personal data between the date of the Personal Data Access Request and the date the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the Personal Data Access Request.

13.5. Data Subjects are only entitled to have access to their own personal data and personal data relating to their beneficiaries, their insured persons, their assignees or their trustees, and not to personal data relating to any other person (unless they are authorized by that person). For the avoidance of doubt:

(a) Data Subjects are not entitled to have access to the information relating to evaluation of their insurance/takaful claims as that information is considered as confidential commercial information;

(b) subject to sub-paragraph (c) below, Data Subjects, other than the policyholders/certificate holders, are only entitled (during the lifetime of such policyholders/certificate holders) to have access to their own personal data and they must first obtain the consent of the policyholders/certificate holders before they make any Personal Data Access Request. The Insurer/Operator has the right to request the Data Subjects to provide evidence to show that such consent has been duly obtained; and

(c) Data Subjects, other than the policyholders/certificate holders (and where such policyholders or certificate holders are deceased persons), are only entitled to have access to their own personal data and/or the deceased persons' personal data (including the insurance policy/takaful certificate) in accordance with the requirements under the applicable laws.

13.6. After the Insurer/Operator has complied with the Personal Data Access Request, a Data Subject may make a request in writing to correct his personal data to the Insurer/Operator if he considers that the personal data is inaccurate, incomplete, misleading or not kept up-to-date ("**Personal Data Correction Request**").

13.7. Where the personal data has been disclosed to a third party during the twelve (12) months immediately preceding the day on which the Personal Data Correction Request is made, the Insurer/Operator must take all practicable steps to supply the corrected personal data that the Insurer/Operator deems necessary to the third party so that the provision of the insurance/takaful and related products and services to the Data Subject is not affected, accompanied by a notice in writing stating the reasons for the correction, unless the Insurer/Operator has reason to believe that the third party has ceased using the personal data for the purpose, including any directly related purpose, for which the personal data was disclosed to the said third party, or if the disclosure to the said third party was by reason of the third party's own inspection of a register containing the personal data and which is available for inspection by the public. The Insurer/Operator shall, to the extent reasonably practicable, retain records or documents evidencing its belief that the third party has ceased using the personal data for the said purpose.

13.8. Notwithstanding what is stated in this Paragraph 13 on the Access Principle, the Insurer/Operator may refuse to comply with a Personal Data Access Request and/or a Personal Data Correction Request in situations that are allowed under the Act, or any relevant subsidiary legislation including regulations, guidelines and rules issued by the PDP Commission, or by any other regulatory authorities. The Insurer/Operator is required to provide notice of refusal and reasons for the refusal, in writing, to the Data Subject within 21 days from date of receipt of the Personal Data Correction Request.

Part D – Processing Personal Data for Direct Marketing

14. The following rules apply to direct marketing exercises performed by an Insurer/Operator:

14.1. Direct marketing activities such as providing information on products and services to Data Subjects is recognized as a legitimate business activity under the Act. The Act defines direct marketing as communications by whatever means any advertising or marketing material which is directed to a particular Data Subject. The application of the law on direct marketing activities vary depending on the medium through which the marketing is delivered, namely, through postal or electronic communications such as SMS/MMS, email, phone call and fax.

14.2. Postal Direct Marketing / Non-Electronic Communications Direct Marketing

The Act does not apply to any marketing done by way of unaddressed mail or flyers, such as those addressed to "*the occupant", "the resident"* or "*the house owner*". This type of mail or flyer, posted through every letterbox on a street, is not direct marketing for the purposes of the Act because it does not involve the use of personal data. However, if the mail or flyer is addressed to a named person and is a form of promotion for a product or service, then it will fall within the ambit of the Act. In these situations, direct marketing may only be carried out if the targeted Data Subject has consented to this. In addition, a Data Subject must be given the right to refuse such processing of his personal data through an "opt-out" option at the time his data is collected.

14.3. Electronic Communications Direct Marketing

Direct marketing done by way of electronic communications include SMS/MMS, email, phone call and fax. An Insurer/Operator may only process a Data Subject's email address or telephone number for direct marketing purposes, if:

(a) the relevant consent has been obtained from the Data Subject to such use of his personal data at the point of collection of his personal data;

(b) the Data Subject is informed that the message communicated is a marketing message and the message is limited to products and services offered by the Insurer/Operator;

(c) the Data Subject is informed of the identity of the direct marketing organisation, purpose of collecting the Data Subject's personal data and the persons to whom such personal data will or may be disclosed to; and

(d) the Data Subject is given a clear and simple method of refusing to consent to the use of his personal data for direct marketing purposes at the time his data is collected.

All marketing communications sent to the Data Subject must contain an "unsubscribe"/"opt-out" option which allows the Data Subject the opportunity to choose not to receive such communications or subsequent marketing messages.

14.4. Online Registration for Marketing Messages or Special Offers

Where a Data Subject registers on the Insurer's/Operator's website to receive marketing messages or news of special offers from the Insurer/Operator, and provides his personal data in doing so, the online registration form must give the Data Subject information about the purpose of, and obtain his consent to allow, the use of his data for such marketing purposes.

14.5. Unsolicited Marketing Messages

If the Insurer's/Operator's business involves the sending of unsolicited marketing messages to the Data Subject, whether via voice calls, text messages (including SMS/MMS) or fax, or sharing of the Data Subject's personal data with third parties outside of the Insurer's/Operator's Group of Companies for marketing and promotional purposes, the Insurer/Operator must check whether the intended recipient has expressly consented to receiving such unsolicited marketing messages from the Insurer/Operator. If the Data Subject has indeed provided such express consent (and has not subsequently withdrawn such

consent), then the unsolicited marketing message can be sent. Note that the unsolicited marketing message must inform the Data Subject that the message communicated is a marketing message and contain an option to unsubscribe from such further marketing messages.

*****End*****