

Frequently Asked Questions about the Code of Practice on Personal Data Protection for the Insurance and Takaful Industry in Malaysia.

1. What are the seven principles outlined in the Code of Privacy Practice in relation to the Personal Data Protection Act?

Number #1 :General Principle

- a. 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, electronically, point of sale systems or over the Internet.
- b. The collection and processing of personal data by Insurers/Operators usually happen at various main stages, such as:
 - pre-contractual stage, including advising, marketing, application or proposal stage;
 - contractual stage, during the term of the insurance policy/takaful certificate; and
 - claims stage.

Number #2 : Notice and Choice Principle;

All Insurers/Operators are required to post an adequate 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.

Data Subjects may contact the relevant Insurer/Operator if they have any complaints, objections or inquiries in respect of their personal data.

A valid deemed consent would arise when the customer/policyholder is informed, made aware of, or knew the purpose for which his personal data would be processed.

Number # 3 : Disclosure Principle;

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.

Number #4 : 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.

Number # 5 : Retention Principle;

- a. 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.
- b. 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.

Number # 6 : Data Integrity Principle

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.

Number #7 : Access Principle

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.

2. What are the types of personal data collected by the insurance/takaful industry?

Generally, the type of data can be classified into :

Non-Sensitive Personal Data:

- (a) name and age;
- (b) home/mailling 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.

3. What is the purpose for the collection of personal data?

Your Personal Data will be used for the following purposes:

- (a) to better understand your needs for insurance protection, provide quotes, enter into and execute your insurance contract, and to set up and administer your policy;
- (b) for underwriting, risk assessment, handling and settling of claims and audit purposes;
- (c) to manage and service the Company's relationship with you and provide you with better customer service including marketing and

promoting of other products and services by the Company and/or its Group;

(d) for data sharing in relation to the administration of your policy.

4. Can an insurance/takaful company collect my information without my consent?

Consent is required for the collection, use and disclosure of personal data. Insurers/Operators would require you to sign on the consent clause for us to process your insurance application. You may choose whether or not to provide your Personal Data to the Company. If you choose not to do so, the Company may be unable to provide you with the services and/or products requested. Hence, it is obligatory for you to provide the Company with your Personal Data when you choose to apply for insurance/takaful cover with the Company.

5. Can I subsequently withdraw my consent ?

You may withdraw consent by letting the relevant Insurer/Operator know in writing. The Insurer/Operator will inform you 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 you.

6. What are my rights as a policyholder (data subject)?

As a customer/policyholder, you may exercise the following:

- Right of access to personal data – you will be informed by an Insurer/Operator whether your personal data is being processed by or on behalf of the Insurer/Operator.
- Right to correct personal data – you can correct your personal data if it is inaccurate, incomplete, misleading or not up-to-date.
- Right to withdraw consent – you can withdraw consent to the processing of personal data.
- Right to prevent processing likely to cause damage or distress – you can request your Insurer/Operator to cease or not begin the processing of your personal data if it is likely to cause substantial damage or distress to you.
- Right to prevent processing for purposes of direct marketing – you can request the Insurer/Operator to cease or not begin processing his personal data for purposes of direct marketing.