## Frequently Asked Questions (FAQ) for Personal Data Protection Act 2010 (PDPA)

**What is Personal Data Protection Act ("PDPA" or the "Act") 2010?**

The Personal Data Protection Act is an act enacted by the Malaysian government in 2010 to protect individual's personal data and it applies to any person who processes and any person who has control over or authorizes the processing of any personal data in respect of commercial transaction.

1. **What are "commercial transactions"?**
   Commercial transactions mean any transaction of a commercial nature, regardless of whether it is contractual. This includes the collection of personal data of potential customers but excludes any information that is processed for the purpose of a credit reporting business.

2. **When was PDPA enforced?**
   The PDPA was enforced on 15th November 2013. For new customers organisations have to comply immediately. However, for existing customers organisations are given 3 months to comply with the PDPA. Please note that customers refer to but not limited to policyholders/certificate holders, non-policyholders insured/non-certificate holders covered, beneficiaries and nominees.

3. **What should I tell the customers if they have any queries before the PDPA has be to be fully complied with?**
   Etiqa is already able to comply with PDPA and can fully execute the customer's rights under PDPA. However, PDPA provided 3 month to fully comply with PDPA for existing customers. For new customers organisations have to comply immediately.

4. **What is personal data?**
   The PDPA defines personal data as any information in respect of commercial transactions that relates directly or indirectly to an individual, who is identified or identifiable from that information or from that and other information in the possession of the individual. This among others includes name, address, identification card number, passport number, email address and contact details.

5. **What is sensitive personal data?**
   The PDPA defines sensitive personal data as personal data consisting of information as to the physical or mental health or condition of individual, political opinions, religious beliefs or other beliefs of a similar nature, the commission or alleged commission of any offence or any other personal data as determined by the Minister by order published in the Gazette. For the collection of sensitive personal data Etiqa is required to obtain explicit consent from the customer.

6. **What is "processing" of personal data?**
   Processing personal data is the act of collecting, recording, holding or storing personal data and carrying out any operation or set of operations on the personal data.

7. **What are the customer's rights under the PDPA?**
   The PDPA gives customers certain rights in relation to their personal data.
   - To access their personal data that Etiqa has about them and to correct this information to make sure that the personal data help by Etiqa is accurate, complete, not misleading and up-to-date.
   - To withdraw their consent for disclosing of their personal data for marketing purposes or any other purposes than for the fulfilment of the service they have subscribed for.

8. **What can Etiqa do with the customer's consent?**
   If a customer gives consent to Etiqa for marketing purposes, Etiqa may send marketing materials to the customer via various channels (e.g. email, letters,phone calls and etc.).

9. **How can a customer change his/her consent?**
A customer may visit any of Etiqa branches, call Etiqa contact centre at Etiqa Oneline 1300 13 8888 or visit Etiqa website at www.etiqa.com.my

10. **What happens if the customer does not give consent?**
If a customer does not give consent to Etiqa for marketing purposes, Etiqa will stop sending marketing material.
However, Etiqa may still use the customer's personal data for purposes of administering insurance policy/takaful certificate or claim against the insurance policy/takaful certificate, fulfilling any other contractual obligations, and fulfilling legal or regulatory purposes.

11. **How does Etiqa obtain the customer's consent?**
For new policyholders, consent will be obtained when they sign up for insurance policy/takaful certificate with Etiqa. For new non-policyholder insured, consent will be obtained by the policyholder. For existing policyholders and the insured, consent will be implied unless they request to opt-out.

Consent information can be captured using the centralised repository called Enterprise Portal Solution.

12. **How long is the cooling-off period for consent?**
After the consent is withdrawn, it takes 14 days before the information is updated in our system.

13. **Why is a cooling-off period for consent required?**
The consent information has to be processed throughout the whole Etiqa organisation and be reflected in the respective IT systems which are used by Etiqa.

14. **After withdrawing consent does the customer still receive marketing material about Etiqa's products and services?**
Etiqa has 14 days to process the consent information throughout Etiqa. Within these 14 days it might be possible for the customer to receive marketing material. However, Etiqa tries to stop sending marketing material immediately but latest after 14 days.

15. **Can a customer request for access to his/her personal data?**
Yes, Etiqa has to provide the customer access to his/her personal data which Etiqa holds about this person. The customer need to contact Etiqa via email to PDPA@etiqa.com.my or please request for and fill in the Access Request Form available at all Etiqa branches/customer service centre. Please note that depending on the information requested, Etiqa may have the right to charge small fee for the processing of any data requested.

16. **Can Etiqa deny the customer's request to access personal data?**
Yes, but Etiqa can only deny the customer's request to access personal data when there is insufficient information to confirm the customer's identity.

17. **Can any other person request access to the customer's personal data?**
A person other than the customer may request access to the customer's personal data in the following situations:

    If the customer is below the age of 18, a parent, legal guardian or a person who is responsible for the customer may request access to the customer's personal data

    A person appointed by the court to manage the customer's affairs may request the customer's personal data

    A person the customer has authorised in writing may request access to the customer's personal data

18. **Does Etiqa have a Privacy Notice?**
    Yes, Etiqa has a Privacy Notice which is available in hardcopy at every branch as well in electronic format online on www.etiqa.com.my

19. **How can I provide more information about PDPA to the customer if he/she requests?**
    Please provide a copy of Etiqa Privacy Notice to the customer.

20. **How does Etiqa safeguard our customers' personal data?**
    We take steps to protect our customers' personal data by maintaining technical and organizational security measures in order to ensure that all information and IT systems are adequately protected from a variety of threats.

21. **What security measures ensure that the customer's personal data is kept secure by other parties?**
    If we disclose our customers' personal data to third parties such as vendors and agents, we must ensure that they have policies and procedures in place to comply with PDPA as well as place or location to secure the customers' personal data.

22. **How long does Etiqa retain its customers' personal data?**
    We will only retain the customers' personal data for as long as necessary to fulfil the purpose(s) for which it was collected or to comply with legal, regulatory and internal requirements.

23. **Does Etiqa send customer's personal data overseas? If yes, why is it necessary to send overseas?**
    In some cases Etiqa may transfer customers' personal data to places outside of Malaysia when it is required to administer your insurance policy/takaful certificate and claims against the policy/takaful certificate, and for the performance of any contractual obligations Etiqa has with its customers.

24. **Does the PDPA cover personal data transferred to those foreign entities?**
    Yes, if the personal data is first processed in Malaysia before transferring to a foreign entity, it will be covered under the PDPA. However, the PDPA will not cover personal data that is only processed outside of Malaysia.

25. **Where does Etiqa collect customer's personal data from?**

    Most of the time, Etiqa collects customers personal data directory from the customers when they sign up for Etiqa's insurance/takaful products or contact Etiqa through various methods (e.g. application forms, emails, telephone calls or conversations with Etiqa staff). Etiqa also collects medical information from doctor of the insured/person covered. For non-policyholder insured/ non- certificate holders covered, Etiqa may also obtain personal data from the policyholder/certificate holder (e.g. employer).

26. **What are the seven (7) Personal Data Protection Principles?**
    The Act set forth a set of seven (7) principles that you need to keep in mind and comply with while processing personal data. The Personal Data Protection Principles are:

    i. **General Principle:** If Etiqa uses customer's personal data for a purpose other than the purpose(s) it was collected for (e.g. when Etiqa wants to use personal data for cross-selling), Etiqa is required by law to obtain customer's consent.

    ii. **Notice and Choice Principle:** Etiqa has an obligation to inform its customer that his or her personal data is being process, the description of the personal data being processed and the purposes of the processing. In addition, Etiqa is also obliged to inform its customers of the rights given to them in the Act (e.g. request access and correct their personal data, contact Etiqa in case of any inquiries or complaints).

iii. **Disclosure Principle:** No personal data should be disclosed to third party (except for disclosure for the original purpose(s) intended at the point of collection) without consent from the customer.

iv. **Security Principle:** Etiqa should take practical steps to implement security measures to protect its customers' personal data.

v. **Retention Principle:** The personal data processed for any purpose shall not be kept longer than is necessary for the fulfillment of that purpose.

vi. **Data Integrity Principle:** Etiqa should take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date.

vii. **Access Principle:** Etiqa customers should be given access to their personal data and be able to correct it.