

BY EMAIL ONLY

Members' Undertaking No. 61
1 April 2015

To: All Ordinary and Associate Members

MU 61/15 - LIA CODE OF PRACTICE FOR LIFE INSURERS ON THE
SINGAPORE PERSONAL DATA PROTECTION ACT (NO. 26 OF 2012)

ACTION:

- 1. FOR ORDINARY MEMBERS' ADOPTION ON BEST PRACTICE BASIS WITH IMMEDIATE EFFECT**
- 2. FOR ASSOCIATE MEMBERS' INFORMATION**

This Code of Practice (Code) sets out best practices for life insurers in Singapore, describing the manner in which the requirements under the Singapore Personal Data Protection Act 2012 (PDPA) may be carried out.

A separate Code of Conduct sets out the minimum standards for tied agents conducting activities on behalf of the life insurer. The Code of Conduct is intended to clarify the duties and responsibilities that a tied agent of a life insurer shall observe in respect of the Singapore PDPA.

Ordinary Members of the Life Insurance Association (LIA) are strongly encouraged to adopt this Code in relation to their handling of personal data in the course of their business.

LIA SECRETARIAT

The Personal Data Protection Act 2012

It governs the collection, use and disclosure of personal data by organisations in a way that recognises both the needs of individuals and organisations.

The PDPA contains 2 main sets of provisions, covering data protection and the Do Not Call (DNC) registry, which organisations are required to comply with.

The PDPA applies to personal data stored in electronic and non-electronic forms.

Scope and Objective of this Code

1. This Code of Practice sets out best practices of life insurers in Singapore on the manner in which they will meet the requirements of the Personal Data Protection Act 2012 (PDPA). Members of the Life Insurance Association of Singapore (LIA) are strongly encouraged to adopt this Code of Practice (Code) in relation to their handling of individuals' personal data in Singapore.
2. In applying this Code, it should be borne in mind that Section 11(1) of the PDPA provides that "In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances." Organisations should consider what is reasonably appropriate when considering how they should meet their responsibilities under the PDPA.
3. This Code incorporates comments and suggestions of the Personal Data Protection Commission with regard to the obligations under the PDPA. This Code is not legal advice or legally binding on the PDPC or any other party. It does not modify or supplement in any way the legal effect and interpretation of any laws cited including, but not limited to, the PDPA and any subsidiary legislation (such as regulations and rules) issued under the PDPA. Accordingly, this Code shall not be construed to limit or restrict the PDPC's interpretation, administration and enforcement of the PDPA. The onus remains with each organisation to assess how the PDPA applies to its circumstances and to ensure that it is in compliance with the PDPA and any other prevailing applicable laws.
4. Unless otherwise stated, terms shall have the same meaning as defined in the PDPA. This Code should be read together with guidelines issued by the PDPC from time to time, particularly where they are relevant to scenarios faced by the life insurance industry.
5. This Code applies to all personal data in the possession or under the control of the life insurer. This includes personal data held in relation to life and group policies, including past proposals and policies. This also includes personal data of any other individual(s) whose claims are being assessed, processed or negotiated in relation to a life insurance policy.
6. In addition to the requirements of the PDPA, life insurers have to comply with regulations and guidelines issued by the Monetary Authority of Singapore ("MAS") specifically for the financial services industries.
7. This Code describes the responsibilities of the life insurer under the PDPA from the perspective of the individual.

The Obligations of the PDPA

8. The PDPA governs the collection, use and disclosure of personal data by organisations such as life insurers and their representatives. The PDPA contains 2 main sets of provisions, covering data protection (DP Obligations) and the Do-Not-Call (DNC) Registry (DNC Obligations). A summary of the DP Obligations is set out in **Appendix A**. You may wish to refer to the PDPA for more details.

Responsibilities of the Life Insurer

1 – Consent Obligation

2 – Purpose Limitation Obligation

3 – Notification Obligation

Overview of when your life insurer may collect personal data from you

9. Pre-application of any policy or service: Representatives of the life insurer interact with you in person or through telephone survey, electronic means (internet, etc), and your personal data is recorded in hardcopy or softcopy modes.
10. Application process of any policy or service: The life insurer may collect personal data from you (e.g. in relation to your health, financial situation and financial goals) in order to make appropriate product recommendations, assess the relevant risk factors, determine the premium levels payable, as well as to comply with other laws that apply to the life insurance industry.
11. Duration of a policy that is in force: You pay the premiums and the life insurer looks after your policy, which is in force. You should keep the life insurer informed of any changes to your personal data such as when you have a new mailing address or telephone number.
12. Making a claim: The life insurer may need to obtain relevant personal data (e.g. medical records) in order to assess whether the claim is payable under the policy, and if so, the correct amount of payment.

1 – Consent Obligation

13. The life insurer will clearly notify you of the purposes for collecting your personal data, how it will be used, and to whom the personal data may be disclosed for such purposes, and seek your consent for the collection, use or disclosure of your personal data for such purposes. This is to ensure that you are informed of the purposes for which the life insurer collects, uses or discloses your personal data. The PDPA requires organisations to collect, use and disclose personal data only for purposes that a reasonable person would consider appropriate in the circumstances.
14. You will be notified of these purposes through appropriate means (e.g. through a statement on the application form). The life insurer must obtain your consent on or before collecting, using or disclosing your personal data for any purpose.

Consent for the collection, use and disclosure of personal data for the following purposes required

15. In order to be able to provide life insurance and related products and services to you, a life insurer would need you to consent to the collection, use and disclosure of the personal data required for the following matters:
 - before you purchase any products or services: the application to purchase and/or provision of advice and product recommendations based on your life insurance needs, as identified

from a Financial Needs Analysis exercise carried out pursuant to the MAS requirement as set out in Notice FAA-N16 Paragraph 34.

- where regular reassessment is conducted after you purchase any products or services: to conduct periodic reassessment of your profile and portfolio to ensure continued appropriateness, to contact you to ascertain if you would like recommendations and advice to be given at the particular juncture, and the provision of advice and product recommendations based on the reassessment. This is carried out pursuant to Paragraph 34 in MAS Notice FAA-N16 and Guidelines FAA-G11 Paragraph 3.3.5.
- underwriting and reinsuring of the risk proposed
- administration of the policy and processing of any claims, requests or transactions under the policy
- compliance with relevant regulations (e.g. MAS regulations) and laws (e.g. tax laws)

16. Examples of personal data that may be collected from you for the matters stated above include but is not limited to:

- Your name, NRIC and/or passport number
- Contact information such as telephone number and mailing address
- Bio-data (e.g. height and weight) and health information
- Employment information
- Financial information
- Investment portfolios
- Personal data of any other individuals (e.g. family members or beneficiaries) to enable the provision of life insurance to you

17. While the PDPA provides that you may withdraw your consent for the collection, use or disclosure of personal data, any withdrawal of consent by you for any purpose(s) that is reasonably required to provide the product or service you have purchased may result in the termination of your insurance contract.¹

18. For example, if you withdraw consent for the use of certain personal data which the life insurer needs to fulfil its obligations to you under the terms and conditions of your insurance contract, the consequences of that withdrawal may be a termination of that contract.

19. The life insurer will inform you of the likely consequences of withdrawing consent when it receives your notice of withdrawal of consent.

Personal Data Collected before the Appointed Day

20. The life insurer may continue to use personal data collected from existing policyholders before the PDPA's appointed day for the purposes for which such personal data had first been collected, so long as these existing uses are reasonable. These existing uses include providing regular updates to you on products and services that the insurer may find to be of interest to you. The appointed day (when the DP Obligations in the PDPA came into effect) was on 2 July 2014.

21. More information on what these existing purposes are will be made available to you by the life insurer.

Telemarketing

¹ Section 16(3) of the PDPA set outs that an organisation must not prohibit an individual from withdrawing consent, although this does not affect any legal consequences arising from such withdrawal.

22. Life insurers will not contact you for marketing purposes at your Singapore telephone number if you have registered your Singapore telephone number with the national DNC Registry. However, some exceptions apply. First, if you have given clear and unambiguous consent in written or other accessible form to receive telemarketing messages from the life insurer and its agents using your Singapore telephone number, the life insurer and its agents may do so even if you are registered with the DNC registry.
23. Second, the life insurer and its agents may also contact you via text (e.g. SMS) or fax in relation to products or services which are related to the subject matter of your on-going relationship with the life insurer and its agents. Depending on the subject of your ongoing relationship with the life insurer and its agents, such products may include general insurance products, for example, hospitalisation policies being marketed to critical illness insurance policy holders.

Withdrawal of Consent

24. After you withdraw consent, the life insurer and its agents and data intermediaries will cease to collect, use or disclose your personal data, as the case may be. Please note that the life insurer is not required to delete your personal data upon receipt of your withdrawal of consent. The life insurer may still retain your personal data if it is needed for legal or business purposes. Your withdrawal of consent also does not affect any legal consequences that may arise from the withdrawal (e.g. termination of the insurance policy).

4 – Access and Correction Obligation

Request for Access to Personal Data

25. You can request for access to your personal data and information about the ways the personal data has been or may have been used or disclosed in the past year by your life insurer by:
- completing and submitting the life insurer's Access Form, or submitting a request in accordance with any other process prescribed by the life insurer; or
 - writing in to the life insurer's appointed data protection officer through the business contact details made available by the life insurer.

The request should contain sufficient information for the life insurer to meet the request.²

26. In both circumstances the life insurer may charge you a reasonable service fee. The fee amount or an estimate will be made known to you promptly before the life insurer starts processing your request. For the protection of your personal data, the life insurer will need to verify your identity before processing the request.
27. The life insurer will verify your identity by, for example, asking to look at relevant identification documents. If the life insurer is unable to verify your identity, you will not be provided access to your personal data.

Situations where Access to your Personal Data may not be provided

28. In certain situations, the life insurer will not provide you with access to your personal data or information about the ways the personal data has been or may have been used or disclosed by your life insurer. For example, the life insurer would not provide access to your personal data or

² Please see the requirements in the Personal Data Protection Regulations 2014.

other information where the provision of that personal data or other information could reasonably be expected to:

- a. reveal personal data about another individual (pursuant to section 21(3)(c) of the PDPA); or
- b. reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity (pursuant section 21(3)(d) of the PDPA).

An example would be the situation where your request relates to a policy for which you are not the policyholder and the policyholder does not consent to the disclosure of his identity. In this case, the life insurer would not provide you the personal data or other information if doing so could reasonably be expected to reveal personal data of the policyholder.

29. If you are requesting for personal data in relation to an Employee Benefits policy under which you are an insured person, the life insurer may ask you to direct your request to your employer instead. If you do not wish to direct the request to your employer, the life insurer will provide you with the personal data you requested (if it is in the possession of the life insurer and the life insurer is able to verify your identity), unless a relevant exception applies.
30. Please refer to section 21(3) and the Fifth Schedule of the PDPA for the list of situations where your life insurer would not need to provide access to your personal data.

Processing of Request

31. On receipt of your access request (and provided all requirements are in order), the life insurer will furnish your personal data within 30 calendar days.
32. If the life insurer is unable to furnish your personal data within 30 calendar days, it will inform you within that 30 calendar days as to the reasonably soonest time by which you will have access to your personal data.

Information to be given

33. The life insurer will provide you with all the personal data and information relating to the use and disclosure of your personal data as specified in your request. The life insurer may ask you some questions when you submit your request to determine the level of detail you would like the personal data and the information to be presented. For example, the life insurer may ask if you are agreeable to receiving a summary of the general uses and disclosures of your personal data.
34. **Appendix B** provides a sample of a response to an access request setting out a summary of an individual's personal data and policy details. **Appendix C** provides a sample of a response to an access request that provides a summary of the general uses and disclosures of an individual's personal data. The actual response you will receive will look different, depending on the specifics of your request.

Situations where corrections to your personal data may not be made

35. In situations where your life insurer is satisfied on reasonable grounds that a correction does not need to be made, the life insurer will annotate the personal data with the correction that was requested but not made.

36. In addition, life insurers are not required to correct or otherwise alter an opinion, including a professional or an expert opinion.³ Life insurers are also not required to make a correction in respect of matters specified in the Sixth Schedule to the PDPA.

Example

Mark is an insured person under an Employee Benefits policy. He received a salary increment and submits a correction request to his insurer to reflect his new salary. The terms of the contract between the insurer and Mark's employer state that any increase in Mark's insurance benefit from the Employee Benefits policy due to increase in salary only take effect on 1st January of the subsequent year, instead of the date of salary increase.

In this case, the insurer may be satisfied on reasonable grounds that the correction does not need to be made, and not make the correction requested by Mark. If it does not make the correction Mark requested, the insurer should annotate Mark's personal data with the correction that was requested but not made.

37. Individuals are strongly encouraged to obtain the concurrence of the policyholder (the party with whom the insurer has a contractual relationship) before requesting a correction of personal data relating to policies which they do not own.

Processing of Request

38. On receipt of your request (and provided all requirements are in order), the life insurer will make the requested correction to your personal data within 30 calendar days.
39. If the life insurer is unable to make the correction within 30 calendar days, it will inform you within 14 calendar days after receipt of your request, as to the soonest practicable time by which the correction would be done.

Sending corrected personal data to other organisations

40. The life insurer will send the corrected personal data within 30 calendar days to every organisation to which the life insurer had disclosed the personal data in the preceding 12 months, unless that other organisation does not need the corrected personal data for any legal or business purpose.

5 – Accuracy Obligation

41. The life insurer will follow appropriate processes and make a reasonable effort to accurately record in its system the personal data provided by you or by another party validly acting on your behalf.
42. Making a reasonable effort will include taking reasonable steps to review the completeness of any submitted forms and or other written documentation, and to verify your identity and particulars against your identification documents.

³ This is set out in Section 22(6) of the PDPA.

43. Life insurers may in many instances assume that personal data collected directly from you will be accurate and complete. When in doubt, the life insurer may ask you to make a verbal or written declaration that the personal data you provided is accurate and complete.
44. In certain situations, the life insurer may request that you provide your personal data again to ensure that its records are current. The life insurer will make a reasonable effort to accurately record in its system the updated personal data provided by you or by another party validly acting on your behalf.

You can help the Life Insurer

45. If there is a change to your contact information such as your home address, email address or telephone number, please promptly update the life insurer, so that the change(s) can be recorded in its system. This ensures that you will continue to receive communications on your policy matters without disruption or delay.
46. Please provide the life insurer with the requested personal data or change(s) in a timely, legible and complete manner.

6 – Protection Obligation

47. The life insurer protects personal data in its possession or under its control by having reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, and other similar risks. The life insurer will establish reasonable practices, which may include establishing internal policies, processes and procedures to restrict access to systems and personal data on a need-to-know basis.
48. In addition to the PDPA requirements, life insurers have to comply with regulations and guidelines issued by the MAS specifically for the financial services industries in relation to the protection of personal data.

7 – Retention Limitation Obligation

49. The life insurer will cease to retain, or anonymise, personal data as soon as it is reasonable to assume that the purpose for which the personal data had been collected is no longer served by retaining the personal data; and such retention is no longer necessary for legal or business purposes.
50. The following table provides an illustration of the minimum retention period for personal data collected for particular purposes.

Purpose for which the personal data was collected:	Minimum retention period
Provision of insurance; and/ or Servicing of an insurance policy that is still in force	Lifetime of the policy
Maintenance of records of consent obtained for telemarketing in accordance with PDPA requirements;	For a reasonable time after the telemarketing was done, when it may be reasonable to assume that it is no longer necessary to

Purpose for which the personal data was collected:	Minimum retention period
and/or Maintenance of internal do-not-call lists	retain documentary evidence of the consent. (assuming there is no longer an intention to telemarket)
Compliance with the MAS Notice on Prevention of Money Laundering and Countering the Financing of Terrorism (SFA04-N02)	5 years following termination of business relations with individual
Compliance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act	5 years following termination of business relations with individual
Retention of information in the event of claim, taking into account the Limitation Act.	6 years following termination of business relations with individual

51. Personal data may be retained beyond the minimum retention period(s) stated above where the retention is necessary for the life insurer’s legal or business purposes.
52. Where personal data is stored for legal or business purposes, the insurer will undertake reasonable security arrangements to protect the personal data (including back-up copies) in accordance with the Protection Obligation under the PDPA. Such arrangements could include, for example, implementing policies to ensure that access to archived documents will be highly restricted and infrequent, or that backup tapes are encrypted and destroyed in accordance with the insurer’s routine archive destruction cycles.

8 – Transfer Limitation Obligation

53. The life insurer will not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.

9 – Openness Obligation

54. Information on the life insurer’s policies and practices regarding the protection of personal data will be made readily available on its website.
55. The life insurer will designate one or more individuals to be responsible for its compliance with the PDPA (“data protection officer”)⁴. The business contact information of at least one of the data protection officers (or authorised delegates) will be made readily available to the public. The data protection officer (or authorised delegates) will be able to answer questions on behalf of the life insurer relating to the collection, use or disclosure of personal data and any other queries relating to the PDPA.

⁴ Legal responsibility for complying with the PDPA remains with the life insurer.

Overview of the Data Protection and Do Not Call Obligations in the PDPA

1 – Consent Obligation

The life insurer will only collect, use or disclose your personal data when you have given your consent, unless collection, use or disclosure without consent is permitted under the PDPA or any other written law.

You may withdraw consent at any point in time for the collection, use or disclosure of your personal data. Upon receiving notice, the life insurer will inform you of the likely consequences of withdrawing consent.

After you withdraw consent, the life insurer and its agents and data intermediaries will cease to collect, use or disclose your personal data. Please note that the life insurer is not required to delete your personal data upon receipt of your withdrawal of consent. The life insurer may still retain your personal data if it is needed for legal or business purposes. Your withdrawal of consent also does not affect any legal consequences that may arise from the withdrawal. (E.g. termination of the insurance policy)

The life insurer may not, as a condition of providing a product or service, require you to consent to the collection, use or disclosure of your personal data beyond what is reasonable to provide that product or service.

2 – Purpose Limitation Obligation

The life insurer may collect, use or disclose personal data about you only for the purpose(s) which a reasonable person would consider appropriate in the circumstances.

3 – Notification Obligation

The life insurer will notify you of the purposes for which it is intending to collect, use or disclose your personal data on or before such collection, use or disclosure of your personal data.

4 – Access and Correction Obligation

Upon your request, your personal data and information about the ways in which your personal data may have been used or disclosed in the past year should be provided to you by the life insurer.

The life insurer is also required to correct any error or omission in your personal data upon your request.

5 – Accuracy Obligation

The life insurer must make a reasonable effort to ensure that personal data about you that is collected by itself or on its behalf is accurate and complete if the personal data is likely to be:

- (i) used by the life insurer to make a decision that affects you; or
- (ii) disclosed by the life insurer to another organisation.

6 – Protection Obligation

The life insurer will make reasonable security arrangements to protect the personal data that it possesses or controls to prevent unauthorised access, collection, use, disclosure, or similar risks.

7 – Retention Limitation Obligation

The life insurer will cease retention of personal data or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the purpose for which the personal data was collected is no longer being served by retention of the personal data and retention is no longer necessary for any business or legal purposes.

8 – Transfer Limitation Obligation

The life insurer will not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.

9 – Openness Obligation

The life insurer will make information about its data protection policies, practices and complaints process available on your request.

The life insurer will designate one or more individuals (“data protection officer(s)”) to be responsible for ensuring that it complies with the PDPA. The business contact information of its data protection officer(s) shall also be made available to the public. However, compliance with the PDPA remains the responsibility of the life insurer.

*Sample response to an access request*⁵

Summary of Personal Data and Policy Details			
Name	<Salutation/Family Name/Given Name>		
Gender			
Identity No			
Date of Birth			
Contact Information			
Telephone Contact	<Home / Office / Mobile - whichever is provided>		
Email			
Residential Address			
Correspondence Address			
Policy Details (where you are the owner)			
Policy Name	Policy Number	Policy Status	Inception Date
e.g. Whole Life	e.g. 12345678	e.g. In Force	e.g. 15 March 1999

⁵This is a sample form for illustrative purposes. The actual response you will receive will look different, depending on the specifics of your request.

Sample response to an access request for information on how personal data may have been used or disclosed within 12 months prior to the date of request⁶

In our usual operations to maintain or service your policy or account, we make use of and disclose your personal data. The main uses and disclosures are listed below.

Summary of General Uses of Personal Data	
	Providing financial advice and recommending product(s), where applicable
	Issuing and administering of your policy, which may include but is not limited to: <ul style="list-style-type: none"> • underwriting and reinsuring of the risk proposed • requesting and collecting premiums • providing regular information about your policy • making changes or updates to your policy • reviewing or renewing your policy • assessing and processing your claim(s) made under the policy
	Compiling statistics for company to design and improve products and services, or industry exercises and studies
	Compliance monitoring and audit reviews
	Complying with all applicable regulations and laws
	Providing general information on product enhancements and services, which are relevant to your needs or in-force policy or policies
	Sending you marketing messages or materials
	Archiving, backing-up or destroying personal data
Summary of General Disclosures of Personal Data	
In the past 12 months, your personal data may have been disclosed to external parties for the following activities	
	To medical organisations, insurance offices or organisations, reinsurers or investigators for underwriting, claims, reinsurance and compliance/audit purposes
	To your financial adviser or representatives for servicing of your plan or policy
	To related companies for the processing and administration of your plan or policy
	To banks, CPF agent banks, credit card companies, other financial institutions or CPF for the collection or refund of any monies due or payable
	To 3rd party vendors engaged by us to perform processes required for the administration of your plan or policy (e.g. data entry, printing and despatch of documents, claims administration, etc) or to perform processes required to send marketing material or messages to you.
	To related companies or 3rd party vendors engaged by us to store and maintain our data and documents, (including storage for business recovery purposes)
	To any regulatory, government and statutory body to comply with applicable, laws or regulation or upon their valid request
	To related company or regional office or head office to comply with Company policies and procedures or upon their valid request

Note

Please note that the actual disclosure form you receive may look very different. Life insurers may develop their own disclosure forms.

⁶ This is a sample form for illustrative purposes. The actual response you will receive will look different, depending on the specifics of your request.