PERSONAL DATA PROTECTION COMMISSION (PDPC) CONSULTATION ON PROPOSED REGULATIONS AND ADVISORY GUIDELINES FOR PERSONAL DATA PROTECTION ACT (PDPA)

Comments (10)	**No comments (9)**
AIA	AXA Life
Aviva	HSBC Insurance
Friends Provident	Life Insurance Corporation (Singapore)
Great Eastern Life & Overseas Assurance Corpn	Manulife
Prudential Assurance	NTUC Income
Standard Life	Royal Skandia
Tokio Marine Life	Transamerica
Generali International	Zurich International Life & Zurich Life Insurance
Swiss Life	

PROPOSED REGULATIONS ON PERSONAL DATA PROTECTION IN SINGAPORE

PART II: ADMINISTRATION OF REQUESTS FOR ACCESS TO AND CORRECTION OF PERSONAL DATA

Tokio Marine Life

1. How do we determine what kind of access requests are chargeable? E.g. issuance of duplicate policy, change of personal data such as address etc. Will there be an industry guide on the kind of access requests which are deemed chargeable?

2. In administering correction requests, does the proposed guidelines allow for individuals to make correction via email/fax? As the proposed position only states that we should accept requests that are made in writing or by any other manner accepted by the organisation. Can this be interpreted that it is up to the organisation to decide on the manner of correction; i.e. can we only insist on our prescribed forms to be completed to perform corrections?

3 How organisations should respond to access and correction requests

AIA

Paragraph 3.7(a) - We'd like to seek clarity on what would constitute "a reasonable opportunity to examine the data" in the event that the organisation is unable to provide personal data requested by an individual.

Prudential

1. Paragraph 3.6 (*Similarly, an organisation is required to make a correction requested in a correction request* …) and paragraph 7.7 (*As proposed, there is no requirement for the organisation to require the receiving party to allow access to or correction of personal data that has been transferred overseas*.)

   Would the obligation to make correction requested be extended to third parties who received the corrected information from the organisation, and the subsequent chain of

the transmission of the personal data? i.e. When Organisation disclose personal data to another Company, i.e. Company A, will Company A be required to make correction to the personal data? If yes, in the event Company A further transmit the personal data to Company B, will Company B be required to make correction to the personal Data?

2. Paragraph 3.7a (*An organisation shall make a reasonable effort to respond to an individual who makes an access request or a correction request as accurately and completely as possible*.) and paragraph 14.5 of the Advisory guidelines on key concepts *(… an organisation may develop (and update periodically) a standard list of all possible third parties to whom personal data may have been disclosed by the organisation instead of a list that specifically relates to the personal data of a particular individual.*)

   The "PROPOSED POSITIONS FOR REGULATIONS UNDER THE PDPA" states that respond to an individual must be as accurately and complete as possible. However, the "ADVISORY GUIDELINES ON KEY CONCEPTS" states that a standard list of all possible third parties to whom personal data may have been disclosed to could be provided. Would such standard list still meet the standard of accuracy and completeness under the PROPOSED POSITIONS FOR REGULATIONS UNDER THE PDPA?

3. Paragraph 3.7 b) ii (*if it is not reasonably possible to provide the requested personal data within 30 days of the individual's request, by the reasonably soonest time. The organisation must inform the individual of when that reasonably soonest time will be within 30 days of the individual's request.*)

   It would be unlikely that organisations would be able to accurately predict the "reasonably soonest time" in cases where retrieval of the requested information is obstructed. As such, propose that organisation be allowed to provide a range of timeframe on the "reasonable soonest time" instead of a pinpointed date.

Standard Life

1. Paragraph 3.5 (*…an organistation is prohibited from providing access to personal data that can threaten the safety or physical or mental health of another individual….)*

   This area involves judgement and Standard Life requests for further guidance from the Authority.

2. Section 3.7, 4 and 5; and Annex A

   Current process at our company:
   1. Standard Life will accept a written Data Access Request (DAR) or a telephone request once the necessary security checks have been completed.
   2. Standard Life will not charge a fee for a DAR. The maximum fee chargeable is €6.35
   3. The timeframe for providing information upon receipt of a DAR request is 40 days.

   Suggestion/Clarification:
   1. The Proposal indicates that the Insurer be flexible in terms of what is an acceptable method of receipt of a DAR. Standard Life requests for guidance/clarification in terms of the acceptable method.
   2. Standard Life requests for the Authority to impose a maximum DAR fee.

3. Standard Life requests for the 30 days timeline to be changed to 40 days or more. Also, clarification required in terms of when the timeline starts i.e. receipt of information and is it based on calender days?

4 How access and correction requests should be made by individuals

Prudential

Paragraph 4.1 *(… through any other manner accepted by the organisation …)* and paragraph 6.2 *(… organisations should also accept requests that are made in writing or by any other manner accepted by the organisation …)*

Would the "any other manner accepted by the organisation" be subject to individual organisations' discretion? What are the "other manners" intended under the proposed regulation? In addition, the regulation should make clear that signatures of individual be required in the request form to ensure confidentiality and integrity of the personal data.

Standard Life

Paragraph 4.1 - Standard Life suggests that organisations should go through appropriate security checks before releasing data to individuals i.e. original ID cards, passports etc.

5 Minimal fee for access request

Prudential

Paragraph 5.1 (*Organisations shall be entitled to charge an individual who makes an access request a minimal fee to recover the incremental costs directly related to the request for the time and effort spent by the organisation in responding to the access request.)*

It would be extremely difficult to determine a "minimal fee" as operating costs differs across companies and industries. Propose for the commission to provide for a range of acceptable "minimal fee" to avoid further dispute of unreasonable "minimal fee".

6 Key considerations in relation to the administration of access and correction requests

Standard Life

Part II Section 6 - No cap on maximum fees have been suggested and Standard Life suggests that a maximum limit be prescribed in the Regulations

Question in relation to the administration of requests for access to and correction of personal data

Question: Do you have any views / comments on the proposed manner in which an individual may make an access or correction request or the proposed positions relating to how organisations are to respond to such requests?

Aviva

1. Personal data of Individuals other than the Applicant or Policyholder

Request for access and correction

These individuals do not have a contractual relationship with the insurer. The Applicant or Policyholder may provide the Insured persons' personal data and also give the consent to collect, use and disclose the information on behalf of these individuals.

As the Applicant or Policyholder is the party giving the consent to collect, use and disclose the information on behalf of these individuals, we feel that these individuals should not have the right of access or correction to their personal data except through the Applicant or Policyholder. Should they wish to access or correct their personal data, such request should be submitted through the Applicant or Policyholder.

Operationally, if insurers are expected to provide access to any individual who is not an Applicant or Policyholder, this process will place a very heavy responsibility on the insurer to perform the verification process on individuals with whom we have no contractual relationship with and exposes the insurer to the increased risk of inadvertently releasing information to an unauthorized party. Even where the personal data information and use is actually released to the correct individual, this information alone or together with subsequent queries by the non policyholder individual may lead to inadvertent release of information sensitive to the policyholder. The policyholder may then choose to seek legal recourse against us for what they would consider to be breach of their confidentiality.
Please note that insurers are expect to safeguard the confidentiality of information based on the Guidelines on Risk Management Practices - Internal Controls issued by MAS 2.2.2 (extract below), Hence, we feel that if we grant access and correction rights to non policyholders, there is a high potential for inadvertent breach of confidentiality of information and the result of such breaches are likely to have severe consequences.

"Policyholder" as used in this context includes individuals who can exercise ownership rights to the policy e.g. Assignee, Trustee.

Guidelines on Risk Management Practices - Internal Controls issued by MAS
2.2.2 The code of conduct should state the ethical values of the institution and prescribe guidelines for employees to observe when discharging their duties. The code should cover areas such as acceptance of gifts and entertainment, conflicts of interest, safeguarding of confidentiality of information, and disclosure of and restrictions on personal investments.

Examples:

Dependent of an individual health plan
Applicants may add their dependents as Insured persons and provide their dependents personal information. Insurers should not need to provide access or correction of personal data for these individual dependents.

Insured Persons, Members or Dependents under a Group Scheme
Insurers should not need to provide access or make corrections for Insured Persons, members or dependents' data under their employer's group policy. If any access or correction is needed for such information, the individual should make the request to access or correct their personal data to their employer. Any corrected data can be subsequently re-submitted to the insurer for updates.

2. Personal data of individuals provided by the applicant or policyholder in order to comply with any regulation

For personal data of individuals other than the Applicant or Policyholder, required to be obtained under the insurance act, FAA or other acts or directives from the authorities that we need to comply with, consent from such third party individuals is not required under Part IV Section 13.(b) of Personal Data Protection Act 2012 (which is at *http://statutes.agc.gov.sg/aol/search/display/view.w3p;ident=7830b12c-09f5-45b0-878a-66d52fc2d422;page=0;query=CompId%3A32762ba6-f438-412e-b86d-5c12bd1d4f8a;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DP%3Btype%3DactsAll#pr13-he-*)

13. *An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless —*
(b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law.

Request for access and correction

We are required not to inform an individual if we had provided personal data to a law enforcement agency under Part V - Section 21.(4) of Personal Data Protection Act 2012.

(4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual pursuant to paragraph 1(f) or (n) of the Fourth Schedule or under any other written law.

As such, for personal data collected, used or disclosed under any written law and already exempted from obtaining consent, the exemption should be extended so that such personal data collected should also be exempt from the access and correction requirements.

It is to avoid scenarios where we inadvertently alert individuals of potential use or disclosure by responding to queries after we provide the individual's personal data to the individual.

Examples:

Beneficial owner
Required to be collected under the MAS Notice on Prevention of Money Laundering and Countering the Financing of Terrorism for identification of parties in control

Bankruptcy information
Captured for the purpose of determining how to administer the policy

Databases for performing Anti-Money Laundering/Combating the Financing of Terrorism (AMLCFT) requirements
Required to fulfill regulatory requirements, e.g. Activa, Worldcheck

PART III: TRANSFER OF PERSONAL DATA OUTSIDE SINGAPORE

Tokio Marine Life

1. Can we interpret that binding corporate rules are applicable for inter corporate transfers with regards to transfer of personal data within the same corporate group?

2. To what extent should the binding corporate rules make reference to transfer of data? In some circumstances, reporting requirements such as complaints, litigation, incidents or adhoc requests relating to client may have to furnish to regional office or head office. Should each circumstance be explicitly stated or a general guide within the corporate rules will do?

7 Requirements for transferring personal data outside Singapore

AIA

It would be good if the Personal Data Protection Commission ("Commission") could clarify whether the obligations described in paragraph 7.5 apply to contracts already in place.

Standard Life

Part III - Section 7.5

Current process at our company:
1. The Irish Regulator (IRE) has no specific requirements with regard to transfer of information outside of Ireland.
2. Standard Life, as per the IRE will retain personal data for 6 years from the termination of the plan.

Suggestion/Clarification:
On point 2 - Standard Life proposed that as soon as it is reasonable to assume that the information is no longer being served or necessary for legal or business purposes.

AIA

Binding corporate rules

The Commission should clarify the meaning of "legally binding", the legal implications and consequences of breach in the context of paragraphs 7.11 and 7.12(c). It is unclear how such internal corporate rules may be made binding on an external party and the legal implications of breach of such rules. The requirement for binding corporate rules to be "legally binding" may be excessive as well.

Friends Provident

Transfer of Data

It will be useful for PDPC to clarify the level of structure and contact details needed in paragraph 7.12(a) of the consultation on the regulation. We will suggest that this point is taken out as it is not useful in terms of according protection to data.

PART IV: INDIVIDUALS WHO MAY ACT FOR OTHERS UNDER THE PDPA

Great Eastern Life & OAC

Part IV - To allow insurers to continue with current practice under S61 of Insurance Act.

8 Exercise of rights and powers of individuals

Friends Provident

Minors, Deceased and Incapacitated

It will also be useful for PDPC to clarify what it means to be "validly acting on behalf of the first individual" in paragraph 8.2(a) of the consultation on the regulation. On this aspect, does paragraph 9.6 to 9.12 empower a person to "validly act" in the instance of deceased policyholders? If so, what about incapacitated policyholders?

In addition is "authorisation in writing" referred to in paragraph 8.2(b), the power of attorney or can the instructions given by policyholders to insurers suffice as authorisation in writing?

Great Eastern Life & OAC

Paragraph 8.2 (b) *Any right or power conferred on an individual and authorized IN WRITING by another individual.*

To allow distribution representatives to make such changes on client's behalf to change address/contact details/email address on behalf of client and insurers verify the change directly in PD with customer eg send letter to old and new address for change of address. Subject to clients must give distribution representatives express authority to make such changes on their behalf, and such authority must be evidenced in writing.

9 Minors and deceased persons

AIA

The Insurance Act allows persons above age 10 to enter into insurance contracts. How would this be consistent with the age of consent proposed by the draft Regulations in paragraph 9.1?

Great Eastern Life & OAC

Paragraph 9.1 (a) (i) & (ii) - The proposals are too complicated and will result in a huge compliance burden. We suggest use of a single age threshold, i.e. Age 18

Paragraph 9.1 (b) *Personal representative or nearest relative of individual deceased for 10 years or less can exercise the rights and powers of PDPA* - Limit to legal representative, including proper claimants, of deceased.

Paragraph 9.1 (b) (ii) *Priority of nearest relatives to an individual* - Limit to legal representative, including proper claimants, of deceased.

Minimum age to exercise rights and powers under the PDPA

AIA

Paragraphs 9.3 & 9.4 *(Minimum age to exercise rights and powers under the PDPA)*

In the context of insurance contracts/products which may be relatively complex for individuals between 14-18 years of age to understand, we'd like to suggest that the organisation be given the flexibility to set a higher minimum age of 18 years if the business model warrants so.

Prudential

Paragraph 9.3 (*As a balance, it is proposed that an individual may exercise rights and powers conferred on him under the PDPA if the individual is 18 years of age or older, or if the individual is under 18 years of age but above 14 years of age and understands the nature of the right or power and the consequences of exercising that right or power.)*

Currently, Insurance Act provides that persons above age 16 years would be regarded as having the capacity to enter into an insurance contract without the need for any consent of his parent or guardian. Given that consent to collect, use of disclose personal data would likely be obtained at the point of insurance application stage, it is proposed that the age of 16 years be applied in relation to insurance contracts, without the additional requirement of understanding the nature of the right or power and the consequences of exercising that right or power.

Priority of nearest relatives to an individual

AIA

Paragraphs 9.9 to 9.11 *(Priority of nearest relatives to an individual)*

The organisation may face practical difficulties in establishing an individual's relations in order to grant priority to the appropriate relative, even if the categories are aggregated. For example, the organisation may not be aware of changes in an individual's marital status (e.g. divorce and remarried) subsequent to a transaction with him, and thus not be able to determine the nearest relative accurately.

Questions in relation to individuals who may act for others under the PDPA

Question 2: Do you have any views / comments on the extent to which minors should be able to exercise rights and powers conferred on them under the PDPA?

Question 3: In particular, do you have any views on the minimum age below which individuals should not exercise their own rights and powers under the PDPA?

Aviva

Proposed approach for minors' rights and powers

We propose to adopt the practice below in dealing with minors with regard to rights and powers under the PDPA to align with the Insurance Act.

Age 18 & above:	same as adult
Age 16-17:	same as adult At this age range, it may not be necessary for the minor to confirm that he understands the nature of the right or power and the consequences of exercising that right or power conferred on him under the PDPA.
15 & below:	No rights and powers

Please see Extract from Insurance Act -

Capacity of infant to insure
58. *-(1) Notwithstanding any law to the contrary, a person over the age of 10 years shall not, by reason only of his age, lack the capacity to enter into a contract of insurance; but a person under the age of 16 years shall not have the capacity to enter into such a contract except with the consent in writing of his parent or guardian.*
[3/2009 wef 01/03/2009]
(2) This section shall be deemed always to have had effect.

Questions in relation to individuals who may act for others under the PDPA

Question 4: Do you have any views / comments on the proposed priority list in relation to individuals that may act for deceased individuals?

Question 5: In particular, do you have any views on the appropriate priority list and/or whether priority should be given equally to all relatives (or to relatives within certain categories such as spouse and children, parents and siblings, etc) for the purposes of the PDPA?

Aviva

Proposed approach for deceased individuals

As there is already an existing framework for the handling the claims of deceased policyholders whereby the insurer will only deal with the correct parties like the proper claimant (or parties acting for the proper claimant), the executor or administrator of the estate. We feel that it will create confusion and complexity and possibly delay in claims processing to introduce a new party on a different basis solely for the purpose of protecting the personal data of a deceased person. As such, we propose that the parties that have the authority to deal with the distribution of assets should also have the authority to protect or disclose the deceased personal information.

ANNEX A: EXTRACTS OF RELEVANT SECTIONS OF PDPA

Section 22: Correction of personal data

Great Eastern Life & OAC

The PDPC should recognise that in some cases, beneficiaries may be named in policies by the policyholder but these beneficiaries should not be treated as being entitled to exercise access and correction rights beneficiary information is confidential. An individual may not even know that he had been named as a beneficiary under a policy. Hence, correcting beneficiary information without proper authorization from policyholder could result in unauthorized disclosure.

PROPOSED ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT

Aviva

Information held on 3rd party systems

(a) Combined databases may be created and updated by various insurers, medical or other organisations for the purpose of administration shield or other types of insurance policies.
(b) Example: ElderShield Register, Mediclaim system
(c) Such combined databases should be exempt from the collection, use, disclosure, access and correction requirements and the participating members should be deemed to be authorised to use the personal information for the original purpose of the system.
(d) Consent for collection, use and disclosure should be obtained by the original data source.
(e) Similarly, access and correction requirements should only be requested from the information source.

5 Personal data

Business contact information

Prudential

Definition of Business Contact Information - Would information other than contact/address information of a vendor given in the context of a Business to Business relationship (e.g. vendor bank account number) be exempted from PDPA in the same light as the exemption for Business Contact Information? This is because such other information of the vendor is obtained in a Business to Business relationship.

6 Organisations

"Agents" who may be data intermediaries

Prudential

In the context of insurance, when an insurance agent solicit personal data from persons for the purpose of entering into an insurance contract, but no such insurance contract was subsequently entered into, would the agent be regarded as "processing" data on behalf of the insurer?

7 Collection, use and disclosure

Great Eastern Life & OAC

Paragraph7.3 (*Collection, use and disclosure – active or passive inclusive*)

1. Names in Corporate Website for Outstanding Maturity is service provided in best interest of customers and is common industry practice, i.e. should be exempted. The information disclosed would be limited to name of policyholder and last 3-4 characters of their ID number.

2. E-greetings - to confirm that non-commercial, non-marketing messages to policyholders even if no consent is obtained, should be exempted. The best practice examples provided are very narrow.

Prudential

Use of Personal Data - Upon a claim event, Insurer might use the medical information to conduct a re-evaluation of the claimant's other policies with the insurer. This is to establish that there is no non-disclosure of existing medical conditions in such other in-force policies. However, the exemption under "evaluative purpose" relates to, inter alia, for purpose of deciding whether to insure any individual or to continue or to renew the insurance of any individual. Please confirm that the use of personal data for such re-evaluation falls under the definition of "to continue" the insurance of the individual.

Part III THE DATA PROTECTION PROVISIONS

10 Overview

Great Eastern Life & OAC

Paragraph 10.2 d)

The guidelines currently do not provide guidance on how detailed companies should respond to customers request for information relating to the use of his/her personal data by the companies. We would like to propose that the following list of generic responses be considered sufficient: "currently, customer personal data presiding PDPA are used for the following purposes:

- Policy servicing (new business underwriting, regular servicing, etc.)
- Communications regarding product and/or services that are relevant to the customer's existing policies and/or needs
- Analytics on an anonymous basis
- Administration (customer service, etc.)

The customers will be able to request for the usage of their personal data during the past one year, meaning as early as 1 June 2013 (one year before the sun rise period ends). The companies' system may not be able to get ready for such request, given the lack of the detailed guidance in the paper.

11 The Consent Obligation

Obtaining consent from an individual

Great Eastern Life & OAC

Paragraph 11.7 - *Organisations should note that the PDPC's default position is that an individual's failure to opt-out would not constitute consent. Failure to opt-out would only be considered consent in certain limited circumstances. Failure to opt-out (or other instances of inaction) may be due to other reasons than the individual's desire to give consent, or it may not be clear how the individual's inaction amounts to consent. Organisations should also*

note that it may be more challenging to prove that consent has actually been given through an individual's inaction.

1. PDPC's default position for obtaining consent should be on an opt-out basis for existing customers. This would facilitate insurers to send mailers to existing customers informing them of the need for them to confirm their existing consent on an-opt out basis. If insurers do not receive a reply within a certain period of time, existing customers will be taken to have given their consent to the as-is/ as usual use of their personal data.

   This would allow insurers to execute on-going operations including:
   - introducing new riders, new insurance products or enhancements to current products
   - informing customers of the status of their existing policies, i.e. maturing policies, and suggesting options for them to reinvest the maturity proceeds.

   Given the high numbers of existing policyholders, this would save insurers the prohibitively high operating costs of sending door-to-door representatives to explain and collect consent from each policyholder. It would also save the policyholders the trouble of having to opt-in should they wish for the continued execution of on-going operations.

2. PDPC should recognise that best practice can extend to obtaining consent from new customers for use of data on an opt out basis The requirement that the staff member handing out the form explains the purpose and the process of opting out to each customer is too onerous and manpower intensive and is simply not practical especially where there are huge customer bases. Bearing in mind that there are already extensive protections under the DNC regime that will prevent contacting customers who have signed up with the DNC via voice, fax or SMS, PDPC should allow for communications to be sent via post on an opt out basis. For the avoidance of doubt, we do not take issue with the existing framework, ie, that customers must have the ability to withdraw consent to marketing use of their data, but only that the best practices prescribed allow for deemed consent on an opt-out basis as well. For example, requirements can include:

   a) the opt out option is expressly provided in the consent form
   b) the opt out option is easy for customers to understand; and
   c) if required, a staff member will be available to explain.

   Reference from other countries who allow such opt out basis:
   - Ireland: www.dataprotection.ie/viewdoc.asp?DocID=905
   - Hong Kong: http://www.pcpd.org.hk/english/publications/files/opt_out_e.pdf

Obtaining personal data from third party sources with the consent of the individual

Great Eastern Life & OAC

Paragraph 11.27 - *Organisations obtaining personal data from third party sources should exercise the appropriate due diligence to check and ensure that the third party source can validly give consent for the collection, use and disclosure of personal data on behalf of the individual (under section 14(4)) or that the source had obtained consent for disclosure of the personal data (under section 15(2)).*

1. Getting friends/ relatives to refer prospects is common prospecting technique adopted by Distribution Representatives.

2. Propose to allow the representative (agent) to verify verbal consent (obtained from referrer friends/relatives) with the prospect/referee when calling him/her the first time (provided that his/her Name is not in DNC Register).

3. If name is in DNC, and express consent, would be required and the call should not be made.

Withdrawal of consent

AIA

Paragraph 11.38 – In the event that an individual's withdrawal of consent would result in the inability of the organisation to continue providing services to him (e.g. it may not be possible to process the individual's data in Singapore separately if all transactions are handled by an outsourced entity outside Singapore), an insurance organisation may face a dilemma as it may not be able to take the necessary actions, even after informing the individual of the consequences (this is because as a basic tenet of insurance, policy contracts do not contain any term or condition which permits the insurer to terminate the policy unilaterally)

14 The Access and Correction Obligation

Access to personal data

AIA

1. Under paragraphs 14.4 and 14.5 of the Advisory Guidelines, an organisation is required to respond to an access request in respect of personal data in its possession as well as personal data that is under its control, and to request for information relating to the use of his personal data. We anticipate the volume of such requests (the right of which is entrenched in law) will result in additional expenses and require significant manpower and resources. Hence, we propose that the Guidelines be expanded to:

   (a) give organisations the right to require all requests to be made in a prescribed format and submitted to such department or division as instructed in the prescribed forms, and to conform to a reasonable process implemented to streamline the processing of such requests; and

   (b) give organisations the right to dictate a reasonable time frame to respond to such requests, especially if the storage and maintenance of such personal data has been outsourced to a third party or is held by an intermediary, and to require the customer to reimburse the organisation for charges levied by such third party for retrieving the required data;

2. With regard to paragraph 14.7 which provides that organisations may charge an individual a fee for access to personal data, the paragraph should be expanded to clarify that the organisation is entitled to impose a fee for each and every request made regardless of whether the requests come from the same person or cover the same personal information over a period of time. The levy of a fee is to discourage customers from taking advantage of the legislation to harass an organisation's employees

repeatedly for information which they might not need or have failed to keep properly, after retrieval or disclosure from the organisation.

Great Eastern Life & OAC

Paragraph 14.5 - *As stated in section 21(1), if an individual requests for information relating to the use or disclosure of his personal data by the organisation, the organisation is only required to provide information relating to how the personal data has been or may have been used or disclosed within the past year. In this regard, an organisation may develop (and update periodically) a standard list of all possible third parties to whom personal data may have been disclosed by the organisation instead of a list that specifically relates to the personal data of a particular individual. The organisation may provide this standard list as part of its response to all access requests that asks for such information.*

In this clause, guidance was given on how organisations can respond to customers request for information relating to the disclosure of his/her personal data by the organisation, e.g. by releasing a standard list of third parties that personal data were disclosed to by the organisation.

However, the guidelines did not provide guidance on how detailed (and in what form) that organisation should respond to customers request for information relating to the use of his/her personal data by the organisation. E.g. is it reasonable if the organisation release a standard and generic set of information in response to such request, such as "personal data were used for evaluative, regulatory compliance and periodic servicing purpose"?

PDPC should also clarify specifically that the access and correction rights when they arise in June 2014 will only oblige organisations to provide access to data held in respect of data subjects in their control or possession at that time, but not necessarily as to how that data was used before June 2014, as organisations are unlikely to be able to modify their IT systems and processes in time to capture use of personal data in the organisation from 1 June 2013 (i.e. 1 year before the end of sunrise period), otherwise they may be at risk of complaints of non-compliance if the organisation is unable to provide information relating to use of customers data during the sunrise period.

Aviva

Access to personal data

To minimize operational requirements to provide information about the ways in which the personal data has been or may have been used or disclosed by the organization within a year before the date of request, we suggest that insurers be allowed to provide a generic list of uses and disclosures for essential use and disclosure of personal data. Each insurer will have their generic list which will cover in general the uses and disclosures required to be issued and to maintain the policy. Insurers will then provide a specific list of uses and disclosures for non essential use and disclosures and this in general will cover the marketing activities performed.

Exceptions to the obligation to provide access to personal data

Great Eastern Life & OAC

Paragraph 14.18 - *Section 22(6) provides that an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion. In addition, section 22(7) provides that an organisation is not required to make a correction in respect of the matters specified in the Sixth Schedule. These include:*
a) opinion data kept solely for an evaluative purpose

Clarification required in this aspect as to whether the personal data of an individual A can be collected, used and disclosed by an insurer without individual A's consent for the purpose of deciding to insure/underwrite a policy for another individual B. Due to the nature of insurance where risks are assessed based on a target group of people with similar background, such exemption should extend to the aforesaid situation. It should also be clarified that the evaluative purpose can also explicitly extend to evaluating claims, as this process involves carrying out independent investigations to verify claims.

Paragraph 14.9 - *The exceptions specified in the Fifth Schedule include the following matters:*
a) opinion data kept solely for an evaluative purpose

It is provided in the PDPA that the requirements relating to the collection, use, disclosure, access to and correction of personal data for “evaluative purposes” will not require consent from the owner of relevant personal data. It is defined in the PDPA that such evaluative purpose includes the purpose of "deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property".

Paragraph 14.9 - The exceptions specified in the Fifth Schedule include the following matters:
j) personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed

Schedule II, III and IV of the PDPA has provided that no consent is required from the owner of relevant personal data if it is for investigation purposes. More clarity is needed in the regulations and guidelines as to whether such investigation includes claim investigation carried out by insurers (through private investigator or not) (the key issue being that the use of the words “associated proceedings and appeals” may suggest investigations in connection with court proceedings). In addition, following from the point made above, sharing personal data with other insurers without relevant consent in the context of claim investigation (eg to assess fraud risks and anti-selection risks) should also be included in the exemption.

Correction of personal data

AIA

Paragraph 14.13 on the correction of personal data should also indicate that if there is a request to correct any data due to the error, inadvertence or negligence of the customer himself, or any developments not made known to the organisation at the time of submission of the original data (which turns out to be obsolete or incorrect), the organisation should be given the discretion to levy a reasonable fee on the customer for correcting such personal data. Such a fee would encourage greater care and responsibility on the part of the customer in furnishing accurate and correct data in the first instance, particularly when such data is relied on by insurers in processing and administering proposal forms and policies and any mandatory reporting functions.

15 The Accuracy Obligation

Great Eastern Life & OAC

Paragraph 15.1 - PDPC to provide industry specific advisory guidelines for insurance companies and their different types of intermediaries on what is reasonable effort

1. Reasonable effort to ensure that PD is accurate and complete if the PD is likely to be used by the organization to make a decision that affects the individual or disclosed to another organization.

2. To have guidelines on what is deemed as "reasonable effort"

17 The Retention Limitation Obligation

Great Eastern Life & OAC

Cease to retain PD or remove the means by which the PD can be associated with particular individuals as soon as it is reasonable to assume that: (i) the purpose for which the PD was collected is no longer served by retention of the PD; (ii) it is no longer necessary for legal or business purposes.

Paragraph 17.1 - More clarity needed on retention period for all data collected for purpose of reviewing anti-selection / anti-fraud.

Standard Life

Section 17 - Make the retention period more specific.

Prudential

(i) Retention of Data

Insurance contracts cover one upon a covered event happening within the period of coverage. There are cases where a claim event happened during the period of coverage but claim was not filed until after the period of coverage expired. In some cases, there is still an obligation on the insurer to pay for these claims notwithstanding that the insurer is only informed of the claim event after the policy has expired. Ceasing to retain such insurance policy records after a period of time would give raise to operational constraint on part of the insurer to verify the claim if the claim was filed after the retention period.

As such, propose for exemption on the retention period for insurance contract and information related thereto, notwithstanding the status of the policy, whether in-force, lapsed, matured, expired etc. Insurer should be allowed to keep information on insurance contracts perpetually as the nature and operation of an insurance contract is largely different from a normal commercial contract.

(ii) Retention of physical copies of data

Some companies might have stored physical copies of data in commercial warehouse which are properly safeguarded. The effort required to anonymise personal data from such physical data storage is huge and significantly outweighs the benefits to anonymise such personal data. Similar constraint applies to destruction of physical copies of data as there involve a process of selecting and identifying which are the copies to be destroyed or retain. Such exercise to select and identify physical copies of documents is also not one-off as the status of policies changes along with time, thus it is not feasible to destroy such documents.

As such, propose for exemption on the retention period for insurance contract and information related thereto, notwithstanding the status of the policy, whether in-force, lapsed, matured, expired etc.

PART IV: OTHER RIGHTS, OBLIGATIONS AND USES

23 Use of personal data collected before the appointed day

AIA

Paragraph 23.5 refers to the rights of the customer to withdraw his consent for the use of his personal data. The paragraph should be expanded to give an organisation the discretion to levy a fee for processing such a change in instructions as the increased costs of manpower to attend to such changes should be borne by the customer and not the organisation.

PART V: THE DO NOT CALL PROVISIONS

AIA

Our concern is the increase in operational costs and the administrative burden to insurers who carry out telemarketing activities. We understand that there may be a fee to check the DNC Registry. Of concern also is the prescribed duration for which the DNC Register has to be checked prior to a specified message (refer to section 43(1) of Personal Data Protection Act 2012). The fee and prescribed duration should be of a reasonable amount and duration respectively. It is not clear for now how the DNC Register actually works, but the DNC Register should be capable of being printed out as at the date of checking as evidence that we have checked the DNC Register within the prescribed duration prior to sending the specified messages.

33 Obtaining consent for sending messages to Singapore telephone numbers

Consent evidenced in written or other form

Great Eastern Life & OAC

DNC (Paragraph 33.4) - *If the consent required under section 43 is not evidenced in written form, it must be recorded in a form which is accessible for subsequent reference. This means that the consent must be captured in a form which can be retrieved and reproduced at a later time in order to confirm that such consent was obtained. Possible forms include an audio or video recording of the consent given.*

Documented consent may not be possible for all situations

Example:

Financial Adviser/ Insurance broker disclose personal particulars to insurers for general insurance quotations. Most of the time, policyholders give verbal consent.

Consent given before the prescribed day

AIA

Paragraph 33.5 - If before the DNC provisions come into operation, an existing customer had neither given express consent for the organisation to send him "specified messages", nor expressly informed the organisation not to send such messages, can this be considered deemed consent, and accordingly, the organisation can send him "specified messages" on or after the date the provisions come into operation?

Other Comments

AIA

For frivolous or vexatious complaints to the Commission (relating to Part VII of the Act on Enforcement - Personal Data Protection Act 2012), the organisation should be entitled to be reimbursed a reasonable amount for its damages, costs and expenses resulting from manpower expended in responding to such complaints and should be entitled to make submissions to the Commission for such reasonable amount to be borne by the customer.

Prudential

Use of Personal Data for corporate governance and assurance purpose - Seek clarification on position of the use of personal data for purpose of internal audits, SOX testing, regulatory supervision etc. The use of these personal data are for corporate governance and assurance purpose, and not purely business, or for administration of policies. Is there a need to have a separate consent of such use of personal data, or if it is acceptable to regard such use under a broader term? If so, please provide guidance on the acceptable broader term.

PROPOSED ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR SELECTED TOPICS

PART II: SELECTED TOPICS

5 Employment

Does an organisation need to seek the consent of a job applicant for the collection and use of his personal data?

Prudential

Paragraph 5.6 (*When an individual voluntarily provides his personal data to an organisation in the form of a job application, he may be deemed to consent to the organisation collecting, using and disclosing the personal data for the purpose of assessing his job application. If the organisation wishes to use the personal data for other purposes, the organisation must then inform the individual of those purposes and obtain his consent, unless relevant exceptions apply.*)

There could be instances when the same set of personal data collected during job application stage (e.g. in application form) are being used for the administration of the employee when he/she joins the company. In this case, would the use of the personal data obtained from the application form (consent deemed for assessing job application) for purpose of administration of the employer/employee relationship be regarded as a non-consented use?

What is the difference between the exception for evaluative purposes and the exception for the purpose of managing and terminating an employment relationship?

AIA

1. In relation to the guidelines on employment in paragraph 5.21, it is clarified that the exception for managing and terminating employment relationships is meant to apply to more administrative operations, such as the use of personal data for payment. However this exception is only applicable to the collection of personal data. There is no equivalent exception for the use or disclosure of personal data. Does this mean that consent must then be obtained for the use/disclosure of personal data collected under the exemption for managing and terminating employment relationships even if the use/disclosure is for the same purpose?

2. In relation to the guidelines on employment in paragraph 5.22 it is noted that there may be instances where the collection of the personal data is necessary for an evaluative purpose and also reasonable for the purpose of managing or terminating the employment relationship and the example of the collection of performance assessments was provided. It was further clarified that an organisation need not obtain consent from the employee nor inform him of the evaluation being carried out but would still required to notify the employee that the performance assessments are to be collected for purposes of managing the employment relationship with him. Why is a distinction made between the 2 when both there are an exemption in the 2nd schedule for both purposes?

MAJOR CONCERNS OF LIFE INSURERS

AIA

1. Transfer of personal data outside of Singapore

   If in future, an organisation adopts a cloud model and data may "sit" in several jurisdictions or even nowhere, or because of organizational changes (e.g. policy data processing is being done in country with lower personal data protection standards) how are organisations suppose to ensure a consistent standard of protection when it depends on the destination country (which is outside the organisation's our control)?

2. DNC - consent from existing customers

   For existing customers, would a one-off communication letter (prior to 1 Jan 2014) informing that the company may use their contact information for sending of marketing messages purposes be sufficient as deemed consent (if the customer did not reply to request for "no sending of marketing messages")?

3. Public awareness

   How would PDPC raise awareness and ensure that the public understands their rights, but more importantly, understand that businesses may sometimes be constrained, so the public needs to have realistic expectations of companies? If this is not addressed at a national level, it would be difficult for individual companies to manage their customer-base.

Operational challenges

1. Leads generated through referrals

   It is a common practice for agent to request their client to provide contact information of a friend(s) [know as leads] to the agent in the client's personal capacity. Such leads provided by the client to the agent are unlikely to have been consented by the leads. The leads may also not be aware that his/her contact information being provided to the agent for subsequent calling on marketing purposes. In such circumstances, how should the insurer apply the PDPDA requirements in terms of obtaining consent and informing on the purposes of the collection?

2. Disclosure on use of personal data upon request

   If the PDPA requires insurer to provide the specific use of the individual personal data in the last 12 months, the current system is unable to tag each and every data activities deployed by the insurer. For example, insurer may generally use the data for experience studies. But the studies may not cover all existing customers. It would be administratively challenging to identify each and every specific use of the individual personal data.

3. DNC – consent from existing clients

We do not have clear consent from our existing customers on sending of marketing messages to their Singapore telephone numbers. If PDPA DNC Provisions require fresh consent to be obtained from existing customers, it would be difficult as most customers would not bother to respond to such requests for consent on receiving marketing messages.

Aviva

Access and/or correction request by individuals who are not policyholders of the insurers

A potential nightmare to insurers as insurers may be faced with many issues.

Firstly, requests may be made to the insurers indiscriminately and possibly on "fishing expeditions". While it is noted that only the personal data of the individuals should be given access and correction, the PDPA also allows individuals to find out how organisations have used or disclosed the personal data in the past 1 year. By revealing the use of the individual personal data, the insurers could potentially be revealing information which a policyholder seeks to protect.

Given the above, we would like to propose that individuals who do not currently have any contractual relationship with the insurers (i.e. who are not policyholders or deemed owners (e.g. assignees, trustees) of the insurers should not be given the right of access or correction.

Friends Provident

Given that the policyholders, lives assured and beneficiaries of a life insurance policy could be different, there should be clarification of the extent of information which can be disclosed or allowed accessed by these different individuals. How will that be interpreted from section 21(3)(c) and (d) of the PDPA?

For example, can a beneficiary ask an insurer to find out which policy is he named as a beneficiary of?

Operational challenges

There could be instances where policyholders or lives assureds are hospitalised, incapacitated or medically not in a position to authorise the disclosure of policy, but for which family members of these individuals need to find out whether there is a life policy taken up with the insurers so they can inform the insurers to follow-up on the claims, or apply for a power of attorney.

Will the disclosure of the above constitute as a disclosure of personal data? No information will be revealed on the amount insured, or type of policies or beneficiaries.

Great Eastern Life & OAC

Employment

Tied insurance agents do not fall within the definition of employee. However, insurers must control their agents conduct in relation to sale of insurance products. Could the exemption to employee consent be extended to apply to tied insurance agents as their insurers is

obligated by regulations to monitor representatives activities relating to sale of insurance products.

Swiss Life

Section 26 PDPA
Advisory Guidelines on Key Concepts - Transfer Limitation Obligation

1. Other than contractual agreements and binding corporate rules to safeguard the transfer of the personal data, would a consent given in writing by the individual to transfer data outside of Singapore be acceptable?

2. Will the Commission be involved in assessing if the organization outside Singapore has complied with requirements prescribed under the PDPA to ensure that the organization outside Singapore provide a standard of protection to personal data transferred that is comparable to protection under the PDPA?

3. Does the Commission require any disclosure reporting of the safeguards or arrangements in-place for such transfers and must the Commission be informed of such transfers of data?

MATTERS THAT ARE NOT EXPRESSLY RAISED IN THE CONSULTATION PAPERS

Aviva

1. Information received on individuals (B2B emails)

   In Group business, it is common to have communications between group client, broker and/or insurers via email and it is possible that personal data of individuals are mentioned in the emails. Such information may not be captured in the Insurer's core system and insurers will face difficulty to provide personal data held by us within such emails as the data is not held or organized in a formalized system. We feel that for such information, the burden or expense of providing such information would be disproportionate to the individual's interest (5th Schedule 1j(iii)). Can the PDPC confirm?

2. Information received on individuals (Other scenarios)

   In Individual business, the intermediaries will often provide a copy of the KYC document which may contain personal information that will not be updated to the insurer's core system e.g. information of family dependents, financial information. It may not be practicable or feasible to create a system to access such information easily. We feel that for such information, the burden or expense of providing such information would be disproportionate to the individual's interest (5th Schedule 1j(iii)). Can the PDPC confirm.

3. Information received on individuals (timing issues)

   Quotation or partly completed application information may have been received by tied agents but not submitted to the insurer's core system. It is administratively challenging to consolidate such information to the insurer's core system. We would like to request for either an exemption of such data until such time an application has been submitted to the insurer.

4. Informal sharing of information between insurers

   Insurers may contact each other to verify various pieces of information. Can the PDPC confirm our understanding of the definitions below as the definitions belong fall under various exempted categories.

   Claims investigations, non disclosure investigations & investigation into fraudulent activity (include AML, ROP etc) qualifies under investigation as defined under Section 2(1). Underwriting qualifies under evaluation purpose as defined under Section 2(1). If consent for above examples is not exempted, insurers will have difficulty managing their operations and preventing fraud.

5. Private Trusts

   Some points to clarify under this item

   a) Can PDPC confirm that all forms of revocable and irrevocable trusts created over an insurance policy can be considered as under private trust?

b) Based on 2nd Schedule 1.l, the exemption is in relation to personal data collected to confer or administer a private trust or benefit plan. As trustees and assignees' personal data are collected to administer a private trust, their personal data are exempted from consent to collect, use and disclose (under 2nd schedule 1l, 3rd schedule 1j and 4th schedule 1s respectively).

c) Based on the same clause above, can personal data for insured persons, dependents, payer etc be considered to be collected for the administration of a benefit plan and as such, exempted from collection of consent to collect, use and disclose. Can the PDPC confirm our understanding of the above otherwise, the insurer may face severe administration challenges e.g. when the insurer receives a notice of assignment or trust, the insurer would not any opportunity to obtain consent from the assignee or trustee for the collection, use of disclosure of their personal data.

6. Withdrawal of Consent

To minimize operational complexities, we would like to request that where an individual submits a request for withdrawal of consent for essential use and disclosure, the insurer will not process the request immediately based on this request. Instead, the insurer will advise the individual of the consequence of such withdrawal of consent for essential use and disclosure and the individual will have to re-submit or confirm their request for withdrawal of consent for essential use or disclosure after the individual had been advised of the consequence of such withdrawal of consent.

7. Status of FIDReC and CASE

Can the Commission confirm that both FIDREC and CASE are considered arbitral institutions?

Also, as the exemptions for arbitral institutions only relate to access and correction, can it be confirmed that consent for collection, use and disclosure are exempted in the Schedules as such cases will be considered as under "investigation".

Prudential

Definition of "Investigation"

PDPA states investigation as an investigation relating to a breach of agreement, a contravention of any written law, or any rule of professional conduct or other requirements imposed by any regulatory authority in exercise of its powers under any written law, or a circumstance or conduct that may result in a remedy or relief being available under any law.

Often, Insurers conduct investigations or review on its representatives, and this involves a review of the cases sold or handled by such representatives, and essentially includes the personal data of customers who purchased policies from such representatives, or from prospects who had liaised with such representatives. Such investigation/ review might not be relating to a contravention of written law. We seek clarification on "any rule of professional conduct" and the scope that investigation/review may be conducted under "any rule of professional conduct".

Generali

Data Protection (Bailiwick of Guernsey) Law 1986

Sensitive data

In the Data Protection (Bailiwick of Guernsey) Law 1986 (mirrors UK Act 1984 and is compliant with EU Directive 95/46/EC), personal data is distinguished from sensitive data.

Relevant filing system

PDPA: Relevant filing system is not mentioned.

Guernsey: "Relevant filing system" - information held on computer and manual information that is organised into a relevant filing system.

Access for correction of an error or omission of personal data is permitted

Guernsey: Provides more reasons for SARs.

Reasonable fee

PDPA: "Reasonable fee" required. This can be disputed and an appeal made to the Commission if the individual finds the sum unreasonable and excessive.

Guernsey: Fee set at £10 (max) - more certain and more advantageous for the data subject requesting the data.

Minors and consent

Guernsey: Statutory age of 18 applied for consent purposes.

PDPA has wider connotations but is still being debated. If the age is taken to be 14 years there would be less certainty as it would have to be proved that the minor understood the powers and consequences of his or her right to powers.

Deceased persons

Guernsey: Does not extend to deceased persons.

Standard Life

Areas addressed in **UK/Ireland Regulations** but not in the Singapore Consultation Papers

1. Dealing with Data Protection Breaches

   The Data Protection Commissioner's 'Breach Code of Practice' states that all errors need to be reported to the Commissioner unless;
   - The error impacts less than 100 customers,
   - The error has been communicated to the impacted customer and
   - The error did not involve any sensitive or financial data

What is a Data Protection Breach?

Any loss of customer information or any instance where customer information is sent or made available to an unauthorised third party.

What should I do if I uncover a Data Protection Breach?

- Notify your manager and the Risk Team in the first instance
- Enter the details of the breach as a Risk Event on ORAC(a Standard Life Risk Management system)
- The Risk Event should include the following information;
  - How many customers have been impacted by the breach?
  - Has the impacted customer been notified and if so, on what date was the customer notified
  - Did the breach result in any financial or sensitive data being lost or accessed by a unauthorised third party
  - What was the process for dealing with the request in the first place and which element of it fell down
  - Does the breach highlight any control gaps in the process or was it a one-off human error
  - Are control enhancements necessary to shore up the process and if so, what is being introduced to ensure this error does not occur again

When should I report the breach & how much information is needed?

Immediately- We may need to notify the Data Protection Commissioner of the breach if it fits the criteria set out above. The Risk Team must notify the Commissioner of reportable data protection breaches within 2 days so it's a very tight window. Our notification must include what happened, why it happened, how we're fixing it and what we're doing to ensure it doesn't happen again.

2. <u>Data protection commission as either a Data Controller or a Data Processor</u>

How is the law enforced?

On an annual basis, entities operating in Ireland register with the Data Protection Commission as either a Data Controller or a Data Processor. What they register as will determine their respective responsibilities in relation to the protection of personal data and information security. (Standard Life International Limited is registered with the Commission as a Data Controller)

The Commission is authorised by the Central Bank of Ireland (Ireland's Financial Regulator) to ensure compliance with the legislation mentioned above. The Commission does this by issuing guidance on how to operate in accordance with the DP Acts. The guidance centres around 8 fundamental principles of data protection. These principles are not an exhaustive list of the requirements imposed upon Standard Life but are provided as a guide. The Principles are listed below;

1) Obtain and process the information fairly
2) Keep it only for one or more specified, explicit & lawful purpose
3) Use and disclose it only in ways compatible with these purposes
4) Keep it safe and secure
5) Keep it accurate, complete and up-to-date
6) Ensure that it is adequate, relevant & not excessive

7) Retain it for no longer than is necessary for the stated purpose or purposes
8) Give a copy of his / her personal data to an individual on request

3. Sensitive/Financial Information

Standard Life must have a system in place to ensure the safety and security of personal data for both employees and customers. The company must ensure that only those who require access to this data (for the stated legitimate business purpose) indeed have access (on a 'need to know' basis).

When dealing with sensitive data (medical information, sexual orientation, work permits etc), tighter restrictions are required in relation to access rights to this information. Standard Life must be able to demonstrate that policies and appropriate procedures are in place to ensure the security of all personal data (sensitive or otherwise).

Staff should be made aware of these policies & procedures and an information security representative should be designated.

CONTACT PERSONS

AIA	Cheryl Koh	Cheryl-KT.Koh@AIA.com
Aviva	Lee How Teck and/or Lim Seok Keng	howteck_lee@aviva-asia.com seokkeng_lim@aviva-asia.com
AXA Life	Jeannie Chua	jeannie.chua@axa.com.sg
Friends Provident	Lawrence Ong	Lawrence.Ong@fpiom.com
Generali Int'l	Veronica O'Brien	veronicaobrien@generali-guernsey.com
Great Eastern Life & OAC	Sainava Bee Bee	SainavaBeeBee@greateasternlife.com
HSBC Insurance	Max Ng	miahiangmaxng@hsbc.com.sg
Life Insurance Corpn	M. Varadarajan	sales@licsingapore.com
Manulife	Nirmala Nair	Nirmala_Nair@manulife.com
NTUC Income	Eileen Chia	nilo@income.com.sg
Prudential Assurance	Si Thiam Teck	Si.Thiam.Teck@prudential.com.sg
Royal Skandia	James Loh	james.loh@royalskandia.com
Standard Life	Hema Chettiar	hema_chettiar@standardlife.sg
Swiss life	Wu Ying Wing	YingYing.Wu@swisslife.com
Tokio Marine Life	Arijit Chakraborty	Arijit.Chakraborty@tokiomarine-life.sg
Transamerica	Silas Tan	silas.tan@transamerica.com
Zurich Int'l Life & Zurich Life Insurance	Linda Ong	linda.ong@zurich.com

Submitted through:
Life Insurance Association, Singapore
18 March 2013