

**PUBLIC CONSULTATION ISSUED BY  
MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS  
ON PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE  
COMMENTS OF LIA MEMBERS**

Summary of Returns:

<b>Comments (8)</b>	<b>No Comments (8)</b>
Aviva	AIA
Friends Provident	AXA Life
Great Eastern Life & OAC	Generali
Manulife	HSBC Insurance
NTUC Income	Royal Skandia
Prudential	Swiss Life
Zurich	Transamerica
	Tokio Marine Life

**PART III: PROPOSED CONSUMER DATA PROTECTION FRAMEWORK**

**A) Key Objectives and Principles**

**Questions in relation to objectives and principles of proposed DP framework:**

**Question 1: Do you have any views / comments on the impact of the proposed DP law on specific sectors? Do you have any suggestions on measures to mitigate this or any other anticipated impact?**

**Question 2: With reference to paragraph 3.8, do you have any views / comments on the concurrent application of the DP law with existing sectoral regulations?**

**Great Eastern Life & OAC:**

- *Question 2*
  - We agree with the concurrent application of DP law with existing sectoral regulations. We would like to clarify on which are the existing sectoral regulations on DP that are more stringent as compared to the proposed DP law. Please advise.
  - Will the stricter standard apply whether under the sectoral regulations or under the DP law?

**Prudential:** *Question 1* – An overly restrictive DP law might hinder trade and business. It is proposed that the DP laws only sets out the principle of DP, and for industry associations to set out specific restrictions / regulations after consultation with the DP Commissioner.

**B) Scope of Coverage**

***Types of Data Covered***

**Questions in relation to the definition of “personal data”:**

**Question 3: Do you have any views / comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?**

**Question 4: With reference to paragraphs 3.15 to 3.16, do you have any views / comments as to whether the proposed DP law should cover the personal data of the deceased? If it should,**

***do you have any views / comments on the proposed approach to the protection of personal data of the deceased?***

**Great Eastern Life & OAC:**

- *Question 3* – The proposed definition is too general and it would be preferable if certain types of personal data are specifically identified as personal data: e.g. NRIC No / passport number, residential address although guidelines can be issued for less common forms of personal data.
- *Question 4* – The proposed DP law should protect the personal data of deceased persons but propose that the period be reduced from less than 20 years to less than 7 years.

**Prudential:**

- *Question 3* – The proposed definition of personal data is too wide. Under the proposed definition, any information pertaining to an individual would be deemed personal data. For example, information is often communicated to employees through the head of department / the employee's manager. Such information could include information particular to that employee such as remuneration, performance reviews, test scores etc. Given the definition of personal data, such communication will no longer be possible unless prior consent for disclosure to the head of department / manager is obtained from employees.
- *Question 4* – It is proposed that DP only covers specific and restricted data of a deceased person. This is because there could be administrative duties to be performed after the demise of a person, and thus personal data might need to be revealed. E.g. family members / law firms checking if a deceased person holds any insurance policy with an insurer, or if the deceased person has any bank account with a bank.

In addition, the proposed protection of deceased person's data of up to 20 years is onerous and could be administratively laborious. It is proposed that the personal data to be retained and tenure of retention be determined by the organisations based on its needs and requirements.

**Zurich:** *Question 4* – We are of the view that the proposed DP law should not cover personal data of the deceased due to administrative complexity which would lead to higher cost and effort. For industries with access to relatively higher sensitive personal data (e.g. banks), there are already sectoral regulations in place to protect personal data.

***Types of Organisations and Activities Covered***

***Questions in relation to the organisations and activities covered by the DP law:***

***Question 5: Do you have any views / comments on the proposed organisations covered by the DP law?***

***Question 6: With reference to paragraphs 3.20 to 3.22, do you have any views / comments as to whether the DP law should extend to organisations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore? Do you have any suggestions as to how the DP law could be implemented if it should apply to such organisations?***

**Friends Provident:** *Question 6* – In relation to paragraph 3.22, we believe Singapore's data protection law should cover only data collection and processing activities carried out by organisations in Singapore, to reduce the possibility of conflicts with similar law in other jurisdictions.

**NTUC Income:** *Question 6* – MICA should consider a fair framework applying to offshore organisations calling customers in Singapore so that there is a level playing field for all organisations, regardless where they are located.

**Prudential:** *Question 5* – It should be clarified as to what extend a person acting in a personal capacity or domestic capacity need not be covered under the DP law. E.g. in the life insurance context, will the provision of a prospect’s name and contact details by an individual to an insurance representative be deemed as acting in a personal capacity or domestic capacity?

It is not clear on how much is regarded as a low annual turnover as described under paragraph 3.19.

## **C) Rules and Exclusions**

### **General Rules**

#### **Questions in relation to the general exclusions from the DP law:**

**Question 10:** *Do you have any views / comments on the proposed general rules under the DP law?*

**Question 11:** *With reference to paragraph 3.35, do you have any views / comments as to whether individuals should be deemed to have given consent for organisations to collect, use or disclose their personal data if they are notified and given reasonable time to opt out but do not?*

#### **Great Eastern Life & OAC:**

- *Question 10* – Are we able to use the information provided in the proposal forms for other purposes such as email blast, SMS broadcast to policyholders and servicing life insurance representatives and also to conduct satisfaction survey? These are part of the services that we make available to policyholders and servicing life insurance representatives in order to address their enquiries and to understand from the customer, the service standards that we are providing.

In the insurance context, personal and policy information is restricted to the policyholder, servicing life insurance representatives and internal staff. If the policyholder had signed an authorisation letter to release such information, are we in compliant with the proposed DP law if we were to release such information to the authorised third party? Currently, we have reservations in doing so with the exception of power of attorney cases as policy information can be sensitive.

Disclosure of personal and policy information will also be made to proper claimants provided that proof of relationship and death certificate is given. We would like to ask if such procedures and requirements are sufficient or if additional measures be required to safeguard the information of the deceased party?

- *Question 11* – If it is clearly provided under the proposed DP law, consumers will not be disadvantaged and organisations will incur much less costs.

#### **Prudential:**

- *Question 10* – It is proposed that general / blanket consent be obtained for all purpose relating to or incidental with the business of ABC rather than specific consent be obtained individually for each purpose relating to the business. A restrictive consent or a need for individual specific consent would result in confusion over the type of consent given. In addition, operationally it will be very challenging to segregate between “deemed consent” and “fresh consent” for existing customers.
- *Question 11* – It is proposed that consent be under the “opt out” arrangement so as not to hinder trade / business and at the same time render protection for data of individuals. In addition, it is unclear as to what constitutes to a “reasonable time”. As such, it is proposed that a statutory

timeline be provided as relying on “reasonable time” would be subjective in each scenario and does not provide a level of comfort for businesses to use such data.

Please also clarify the lead time given for organisations to execute customers' instructions to withdraw his consent for use of his personal data. For marketing campaigns (such as direct mail, email or SMS, though non-exhaustive), data would be cut as at a certain date while the execution of the campaign is 2 - 3 weeks thereafter. Customers may write in to withdraw their consent during the window period and it may not be possible to stop the mail / email / SMS in time.

### **Rules on the Collection, Use and Disclosure of Personal Data**

#### **Questions in relation to the proposed rules on collection, use and disclosure of personal data:**

**Question 12: Do you have any views / comments on the proposed rules on collection, use and disclosure of personal data?**

**Question 13: Do you have any views / comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organisations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organisation? Are there any other exceptions that should be provided?**

**Question 14: Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined at paragraphs 3.60 to 3.61?**

**Friends Provident:** *Question 12* – In relation to paragraph 3.41, we believe that a specified contact information of the organisation would serve the purpose better than that of a contact information of an officer or employee. A valid group mailbox which is maintained and accessed by a number employees in the organisation means the concerns of the individuals will be looked upon and managed even if a specific employee is absent from the organisation. In relation to that point, it is onerous to have to designate one or more individuals to be responsible for the DP Act as stated in paragraph 3.38. Not all Acts or subsidiary legislations require designation of persons responsible, and it is challenging why the DP Act should receive priority above others. We agree that the organisation, as the legal person, should be responsible for the DP Act.

#### **Great Eastern Life & OAC:**

- *Question 12* – For paragraph 3.41, before collecting an individual's personal data, an organisation shall disclose to the individual, verbally or in writing the purposes for collection of the personal data. As such, when customer provides personal data in the proposal forms, is it necessary to have additional disclosures / declarations statement in proposal & application forms to inform or obtain agreement from the customer for the collection of data? Would we need to extent this to feedback and survey forms, where information is collected mainly for feedback on our services and personal data disclosed is merely for identification purposes?
- *Question 13* – Collection, use and disclosure of an employee's personal data would be acceptable for the purpose of identifying him as an employee of the organisation, an exception to the general rule would be acceptable.

What is the retention period for the insurance industry to maintain policy records necessary for business or legal purposes? For policy and customer records, we would suggest to follow the retention period as required by the industry. For other such as feedback or survey forms, perhaps a time frame of 3 to 4 years will be sufficient.

- *Question 14* – No objections as financial institutions are already bound by the MAS Outsourcing Guidelines to protect the personal information of the customers if such information is required to be provided to service providers in an outsourcing arrangement.

**NTUC Income:** *Question 12* – MICA should clarify if insurance companies are able to circulate personal particulars of insurance policyholders within the insurance industry when a policyholder submits a claim or during a policy application to their insurer. Currently, it is a common practice in the insurance industry to share insurance policy information to enable insurance companies to verify what was declared in the insurance claims or insurance policy application form. We would therefore appreciate if MICA can define the word “investigation” in Paragraph 3.42 more clearly, to explain whether this would include investigating an insurance claim that is being submitted or a new insurance application submitted by an applicant. If yes, does that mean that insurers can share information about the claimant or applicant without first seeking his consent (i.e. Paragraph 3.41). E.g. Mr Tan files a claim with Insurer A. Insurer A checks with Insurer B and C to find out if Mr Tan has submitted a claim as well with them and the details of any medical reports already obtained by Insurer B & C. Must Insurer B & C seek Mr Tan’s consent before releasing such information to Insurer A?

**Prudential:**

- *Question 12* – Similar to our response to Question 10
  - It needs to be clarified if transfer of data between related companies is allowed or would constitute to a breach under the DP law, taking also into consideration that certain related companies might be outside of Singapore.
  - The legislation should also exclude from the framework data that is shared amongst group companies and professional advisers on strict confidentiality basis.
- *Question 13* – See our response to Question 12
  - To consider the sharing of information specific / necessary for specific industry (e.g. LIA centralize database, GIA database etc).
  - It is proposed that the exception of DP laws to employee extends in the same manner to insurance representatives as well.
- *Question 14* – Yes

**Rules on Accuracy, Protection and Retention of Personal Data**

**Questions in relation to the proposed rules on accuracy, protection and retention of personal data:**

***Question 14: Do you have any views / comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67?***

***Question 15: With reference to paragraph 3.67, do you have any views / comments as to whether organisations should be required to specify the retention period when collecting personal data?***

**Great Eastern Life & OAC:**

- *Question 14* – Given that the personal information is directly provided by our customers, would insurance companies not be required to ensure that the personal data of customers is reasonably accurate and complete? As for retention of personal data of policyholders, given the nature of the insurance policies especially life policies, we would need the personal data of the policies as long as the policies are still in force which could be for a few decades.
- *Question 15* – Given the nature of life insurance policies, it would be natural and reasonable for policyholders to assume that the personal data given by them to insurance companies would be retained for as long as they remain as a customer of the insurance company. Hence, we do not see the need to specify a retention period for purchasers of insurance policies.

**Prudential:**

- *Question 14* – The requirement to ensure data is accurate should not apply in events where a prospective policyholder makes an offer to the insurer for the application of an insurance policy. The onus to provide accurate data should lie on the policyholder since insurance is a contract of utmost good faith.
- *Question 15* – It is proposed that the personal data to be retained and tenure of retention be determined by the institution based on its needs and requirements and organisations need not specify the retention period when collecting personal data. As such, it is proposed that the disclosure of the retention period should be in a broad and generic term, rather than a specific timeline.

In the case of long term contracts, the personal data provided could be relied upon as evidences in future and thus having a restrictive retention period might not be feasible.

**Zurich:** *Question 15* – We are of the view to not want to specify the retention period at the point of collecting the data. Different industries may need to comply with other data retention legislation / regulations apart from the DP law. If these legislation / regulations change in future, it would then cause additional administrative cost and effort to update the existing clients if we have already disclosed a different retention period to them.

From a client perspective, most would not be overly interested in knowing the retention period as long as they have the assurance that their personal data is protected under the necessary legislation / regulations.

**Rules on Access to and Correction of Personal Data**

**Questions in relation to the proposed rules on access to and correction of personal data:**

**Question 16:** *Do you have any views / comments on the proposed rules on access to and correction of personal data?*

**Great Eastern Life & OAC:** We have no objections to charging a reasonable fee to customers who wish to correct their personal data although currently we do not charge a fee.

**Prudential:** It might be administratively laborious to inform third parties of the change in personal data and the third parties might not require such updates. In the case of bancassurance model for example, a customer might wish to keep separate correspondence addresses for his banking and insurance needs.

In addition, it is proposed that the type of data that are assessable to individual and subject to amendment by the individuals under paragraph 3.69 be defined. Accordingly, it is proposed that non-material information should not be covered under the DP law.

**PART IV: IMPLEMENTATION**

**A) Penalty and Enforcement Regime**

**Questions in relation to the proposed penalty and enforcement regime:**

**Question 17:** *Do you have any views / comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?*

**Question 18: Do you have any views / comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views / comments on the criteria for breaches that would warrant financial penalties?**

**Great Eastern Life & OAC:** *Question 18* – As long as the criteria for breaches is very clear, we have no objections to the proposed penalties for contravention of the proposed DP law as long as mere negligence and unintended inadvertence in breaching the proposed DP is not punished with monetary penalties.

### C) Transitional Arrangements

#### *“Sunrise” period*

**Questions in relation to transitional arrangements:**

**Question 19: Do you have any suggestions on specific guidelines that the DPC should provide to help organisations achieve compliance with the DP law?**

**Prudential:** Industrial associations should self regulate on DP regulations, rather than relying on strict DP laws, which could impede trade and businesses.

#### *Existing personal data*

**Questions in relation to transitional arrangements:**

**Question 20: With reference to paragraphs 4.11 to 4.14, do you have any views / comments as to whether a one to two year “sunrise” period would be appropriate?**

**Question 21: With reference to paragraphs 4.15 to 4.19, do you have any views / comments on the proposed treatment of existing personal data?**

**Question 22: Are there certain organisations that may require different transitional arrangements?**

#### **Aviva:**

- *Question 20* – Sunrise period of 2 years would be appropriate.
- *Question 21* – For existing customers, Company should be given a right to call unless client specifically states otherwise or client included in the Do-Not-Call (DNC) register.

**Great Eastern Life & OAC:** *Question 20* – It would be preferable to have at the very least a 2 year "sunrise" period to enable organisations to comply with the proposed DP law.

#### **Prudential:**

- *Question 20* – Sunrise period should be at least 2 years or longer.
- *Question 21* – It is proposed that all activities incidental to the business should be regarded as deemed consent for such activities to be carried out. Accordingly, consent should not be overly restrictive. Further, individuals whose personal data has already been collected should be deemed to have consented to the use of such data, even for new purposes, once the proposed legislation is in place. An opt-out exercise should apply to such cases.

## PART V: NATIONAL DO-NOT-CALL REGISTRY

### ***Questions in relation to proposed National Do-Not-Call registry:***

**Question 23: Do you have any views / comments as to whether a National Do-Not-Call registry should be set up in Singapore?**

**Aviva:** Yes, there should be a National Do-Not-Call (DNC) registry in Singapore. Consumer should be able to self-register to the DNC Register on a renewable term basis (e.g. 24 months) with a choice of DNC to be imposed on specific industries.

**Friends Provident:** In relation to paragraph 5.5, a national DNC registry will cause compliance cost to be significantly higher because there has to be constant referencing to the national registry before advertisements are sent to individuals. If an organisation already maintains its own DNC registry and protection is given to how personal data is obtained and used, then a national DNC registry may be duplicating the protection given by these measures. Hence we would urge a rethink of having a national DNC registry.

**Manulife:** With reference to Part V, Manulife is of the opinion that the Registry should operate in the same way as the UK model -- when a member of the public request that they want to opt out of any kind of unsolicited calls their names will not be included on any list sold to a tele sales company or in our case to agents.

The onus is on the companies selling the lists to make sure that the lists do not contain names that have been registered with the national system.

Secondly this will not preclude us from contacting existing clients or those who are introduced to us by referral.

Thirdly, we need to address the issue of registrants changing phone numbers and the impact of re-circulated numbers as practiced by telcos in Singapore.

**NTUC Income:** On registering under the National DNC registry, we would like to highlight the following points:

- (a) It does not make commercial sense for the national DNC registry to apply to organisations if they have a business relationship with the individuals concerned. It is common practice for organisations to contact their customers on a periodic basis to provide them with product or information update. If the customers do not wish to be contacted, they would already have requested to be registered under the individual company's DNC list.
- (b) MICA must consider giving individuals the option to select the sector / industry which they do not wish to receive information from. It does not make commercial sense for the registry to apply across all sectors. Given that all telemarketing operations of general insurers are guided by MAS Notice 211, telemarketing activities conducted by the organisations comply with the MAS regulatory requirements on Fit & Proper Criteria. It thus seems harsh to penalise some industries for bad conduct of other industries.
- (c) We suggest there must be a cost effective and hassle free of downloading the DNC registry. We must be aware that there is a lead time between the date of registration and the date of calling. Organisations should not be penalised if violations occur during this period.

**Prudential:** A National Do-Not-Call registry is good but there are considerations such as how fast would the registry be updated to reflect the latest Do-Not-Call list. It would also be important to know if a DNC list covers all purpose of a call, or if it only applies to specific category of calls or specific sectors, such as "not to be contacted for unsolicited calls". A company should be able to continue calling the number if the holder of such number is an existing customer of an organisation and calling such customer is necessary. In addition, would consent given would be superseded by subsequent inclusion under the Do-No-Call Registry?



## CONTACT PERSONS

Aviva	Stanley Yeo   stanley_yeo@aviva-asia.com
Friends Provident	Lawrence Ong   Lawrence.Ong@fpiom.com
Great Eastern Life & OAC	Adeline Long   adelinelong@lifeisgreat.com.sg
Manulife	Margaret Ho   Margaret_Ho@manulife.com
NTUC Income	Peter Teo   peter.teo@income.com.sg
Prudential	Tee Swee Vien   Tee.Swee.Vien@prudential.com.sg
Zurich	Max Ng   max.ng@zurich.com.sg or Paul Ballam   paul.ballam@zurich.com.sg

**Submitted through**  
**Life Insurance Association, Singapore**  
**19 October 2011**