PUBLIC CONSULTATION ISSUED BY MINISTRY OF INFORMATION, COMMUNICATION AND THE ARTS

PROPOSED PERSONAL DATA PROTECTION BILL

SUBMISSION BY THE STARHUB GROUP TO THE MINISTRY OF INFORMATION, COMMUNICATION AND THE ARTS

30 APRIL 2012

Contact	:	Veronica Lai / Thng Shin Min
Address	:	StarHub Ltd 67 Ubi Avenue 1 #05-01 StarHub Green Singapore 408942
Phone	:	6825 5136 / 6825 5192
Email	:	veronical@starhub.com / shinmin.thng@starhub.com

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

StarHub welcomes the opportunity to provide feedback on the proposed Personal Data Protection Bill by the Ministry of Information, Communication and the Arts ("MICA") and supports the need for legislation to keep pace with developments in the industry and with market conditions.

The key areas of StarHub's response to the proposed Personal Data Protection Act ("PDPA") are as follows:

(i) The proposed PDPA should not apply concurrently with existing sectoral regulations, failing which there could be uncertainty and confusion. Instead, we submit that where the industry is subject to sectoral regulations, these should take precedence over the proposed PDPA.

(ii) It would not be practicable to restrict the consent obtained from an individual only to what is necessary to provide the product or service. This approach is unduly narrow and restrictive. Instead, the touchstone should be a reasonably scoped consent.

(iii) An "opt-in" approach would be onerous and impractical, especially in the case of organisations which already have a large consumer base. Instead, we propose that where organisations are subject to sectoral regulations which currently provide for an "opt-out" approach, this should take precedence over the proposed PDPA.

(iv) It would not be practicable to require organisations to keep track of the duration in which personal data has been used and the ways in which personal data has been used, especially for organisations which have a large consumer base. Instead, we propose that it would be sufficient for organisations to abide by its internal retention policies. During the period of retention, the organisation would be bound by the proposed PDPA and/or sectoral regulations.

(v) The proposed penalty and enforcement regime under the PDPA is too harsh. Instead, we propose that financial penalties should only be imposed on a step-up basis, wherein a harsher penalty is imposed only in instances of repeated violations by organisations.

(vi) As regards the proposed National Do-Not-Call ("DNC") Registry, telecommunication licensees should not be required to provide the list of terminated numbers to the DNC registry on a monthly basis. The costs of requiring telecommunication licensees to comply with this requirement are likely to outweigh the costs of adopting an alternative approach i.e. to allow individuals to make enquiries on the status of their own phone numbers, for free or at a nominal charge. Further, the proposed penalty on telecommunication licensees for failure to provide the list of termination numbers is too harsh.

(vii) The proposed penalty and enforcement regime is too harsh and does not commensurate with the potential inconvenience experienced by a consumer who has received a marketing message despite being listed on the registry. Instead, we propose that financial penalties should only be imposed on a step-up basis, wherein a harsher penalty is imposed only in instances of repeated violations by organisations.

StarHub is pleased to provide its detailed comments on the proposed PDPA in the following section.

2. COMMENTS

General Provisions on Data Protection

MICA's position in the PDPA	Comments
PDPA will maintain a baseline regime that applies to all private sector organisations, including small companies that have low annual turnover, to ensure a minimum standard of DP across the private sector. (Paragraph 2.11) However, the provisions of the PDPA also state: s.4(7): "To the extent any provision of this Act is inconsistent with any provision of other written law, the provision of the other written law shall prevail." s.15: "An organisation shall not…collect, use or disclose personal data about an individual unless…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."	We submit that the baseline approach does not create sufficient certainty for compliance. The PDPA continues to maintain the position that the data protection regime applies concurrently with existing sectoral regulations. As there may be areas of overlap between the proposed data protection regime and sectoral regimes, this may result in confusion as to which standard should apply and an organisation may be subject to duplicate penalties and sanctions under both regimes. Thus, we reiterate our position that the data protection regime should not apply concurrently with existing sectoral regulations. We submit that the PDPA should adopt a clear position that where organisations are subject to existing sectoral regulations which govern the use of personal data, the sectoral regulations should take precedence. This would avoid conflicts and discrepancies between the sectoral regulations and the data protection regime. On this note, we would suggest that an approach similar to the competition law regime would be more practical. The competition law regime provides that the provisions of the Competition Act shall not apply where another regulatory authority has jurisdiction.
MICA maintains its proposal to prohibit organisations from requiring an individual to consent to the collection, use or disclosure of personal data, as a condition of supplying the product or service, beyond what is reasonable to provide the product or service to that individual. MICA clarifies that this does not override existing regulatory or statutory requirements that organisations have to comply with. Organisations may still collect additional data without consent if required or authorised under other written laws. This applies when collection, use or disclosure is expressly permitted rather than mandated by law. (Paragraphs 2.42, 2.43 and s.15, PDPA)	We reiterate our concerns regarding the concurrent applicability of sectoral regulations and the data protection regime. In the event organisations are required to adhere to both regimes, we submit that it would be unduly narrow and restrictive to confine consent to what is necessary to provide the product or service. This will restrict innovative options open to consumers, given that new products and services are always evolving. The data protection laws should consider the need to meet customers' demand for new and innovative services. Our legislative regime should not stifle consumer choices made with their knowledge and consent.

MICA's position in the PDPA	Comments
	We submit that the correct touchstone is to require consent to be "reasonably scoped" and not "overly broad".
For the purposes of obtaining consent, organisation shall inform the individual of the following: (a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer the individual's questions about the collection, use or disclosure on behalf of the organisation. Organisations should ensure that the purposes be reasonably scoped and not overly broad. (Paragraph 2.46 and Section 22, PDPA)	We suggest that it would be sufficient for such information to be included in the relevant terms and conditions between the organisation and the individual. This would be consistent with the approach taken by MICA in the lucky draw scenario at Annex C of the Consultation Paper.
Consent should not be deemed if individuals do not opt-out when they are notified of an organisation's intent to collect, use or disclose their personal data. This is because individuals may be unfairly subject to serious risks e.g. they may be unable or unaware of the need to object, or of the implications of not objecting. Failure to "opt-out" will not be deemed consent. (Paragraph 2.50)	We propose that where sectoral regulations provide for an "opt-out" approach for obtaining consent, this should take precedence. s.15 of the PDPA states: "An organisation shall not…collect, use or disclose personal data about an individual unless…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." Section 15 of the PDPA does not override existing laws or sectoral regulations. Accordingly, where the sectoral regulations provide for an "opt-out" approach, it should be made plain that organisations would not be in breach of the PDPA if they are in compliance with their sectoral regulations.
Organisations should be required to obtain fresh consent from the individual if the personal data collected was to be used for a different purpose than that for which consent had been given. (Paragraphs 2.84 and 2.85)	We submit that this approach is narrow and unduly restrictive as it would be difficult to determine whether consent has been given for a particular purpose. Rather, we suggest that it would be more practicable to adopt the approaches taken under the IDA Telecom Competition Code and MDA

MICA's position in the PDPA	Comments
	Competition Code, which allow organisations to collect personal data and seek consent from consumers for broader purposes. Consumers should have the freedom to make informed decisions.
PDPA will allow individuals to find out how organisations have used, or are using the personal data collected, correct information that may be inaccurate, or seek redress for suspected breaches of the PDPA. Upon request of an individual, organisation shall, as soon as reasonably possible, provide the individual with his or her personal data in the custody or under the control of the organisation, and information about the ways in which the personal data has been or may have been used by the organisation. (Paragraph 2.92) Organisations can be allowed to charge a reasonable fee on a cost recovery basis. There will be no prescribed fee, but organisations shall give the applicant a written estimate of the fee before providing the service, and can require the applicant to pay a deposit. (Paragraph 2.97) Organisations should respond to applications no longer than 30 days from the time of request, unless reasonable justifications can otherwise be shown. (Paragraph 2.98)	We submit that the time period for organisations to respond to such requests should be left to the organisations to determine and advise the individuals. Each organisation differs and the size of customer base also differs. It would be better to require that organisations respond within a "reasonable period" than to prescribe specific timing.
Organisations would need to delete or anonymise data as soon as it is reasonable to assume that the purpose for which the data was collected is no longer being served by its retention, and retention is no longer necessary for legal or business purposes. Where organisations use an individual's personal data to make a decision that directly affects that individual, the organisations shall retain that personal data for at least a year after using it, so that the individual has a reasonable opportunity to obtain access to it. (Paragraph 2.111)	We submit that there is no need to over-regulate and prescribe how organisations to keep track of the duration in which personal data has been used and the ways in which personal data continues to be used. We would suggest that it would be sufficient for the organisation to abide by its internal retention policies, and to impose a standard of reasonableness.

MICA's position in the PDPA	Comments
MICA is of the view that where a particular incident may constitute a breach in both regimes, it would be preferable that the organisations be subject to the investigative and enforcement actions of one regulator. The PDPA will therefore provide the DPC with the powers to refer an incident to another regulatory agency, if necessary. (Paragraph 2.122)	We submit that this approach will potentially lead to confusion and uncertainty as to which standard should apply, as organisations may be subject to the penalties and sanctions of either regimes, or both. We would suggest that the legislation clearly provide that where organisations are subject to existing sectoral regulations, the organisation would only be subject to the penalty and enforcement regime under that applicable sectoral regulation. There is precedent to this approach, by way of the competition law regime. Clarity in legal obligations should be paramount; Singapore has a global reputation for respect of the Rule of Law.
Sunrise period should be no less than 18 months for all organisations from the time the PDPA is enacted. • DPC will conduct awareness-building activities for both businesses and consumers, in relation to their rights and obligations under the regime, targeted at enhancing organisations' ability to comply. • Guidelines will be published on various issues that may assist with organisations' efforts to comply with the PDPA. (Paragraphs 2.134 and 2.135)	We reiterate our position that the "sunrise" period should be 2 years. 18 months may not be sufficient for organisations to modify their customer management systems to comply with requirements of the PDPA. Organisations, regardless of size, will need to expend significant time, money and resources to educate their staff and ensure they are able to comply with the PDPA when it comes into effect.

Provisions on the Do-Not-Call Registry

MICA's position in the Proposed Data Protection Act (PDPA)	Remarks / StarHub's further submission, if any
The DNC Registry will be maintained by the DPC.	As regards the implementation of the DNC Registry, we propose that MICA clarify the following: • Who will bear the costs of the DNC Registry?
MICA proposes that telecommunication licensees will be required to provide the DNC Registry with a list of terminated Singapore telephone numbers at a regular monthly interval. The monthly intervals will ensure that such numbers are removed from the DNC Registry before they go back into circulation. The DPC will pay prescribed fees to the telecommunication service provider for each terminated Singapore telephone number. (Paragraph 2.164) Further, telecommunication service provider who does not comply with this requirement shall be liable on conviction to a fine up to $10,000 per incident. (Sections 46, PDPA)	We reiterate our submission that it would be onerous and impractical to require telecommunication licencees to provide the list of terminated numbers to the DNC Registry: • such information constitutes commercially sensitive information, which telecommunication licencees are unable to provide to the DNC Registry. • The costs involved in extracting the list of terminated numbers would not be limited to the costs of extraction only, as telecommunication licencees will have to incur costs to set up and maintain a system to generate the terminated numbers on a monthly basis, in accordance with such form and manner prescribed by the DPC. Such costs should be passed on to the DPC. • This requirement would make the regime needlessly complicated. As previously submitted, we propose that the DNC Registry should instead allow individuals to make enquiries to the DNC Registry on the status of their own phone numbers, for free or at a nominal charge. Individual consumers would have an interest to know the status of their own phone numbers. This would also reduce the work needed on the DNC Registry's part to check and/or update the list each time they receive a list of terminated numbers. The cost of allowing individuals to check the status of their own numbers is likely to be lower than the costs which may be incurred by organisations in providing the list in accordance with the PDPA. Further and in the alternative, we submit that the proposed penalties to be imposed on telecommunication licencees for failure to provide the list are too harsh and punitive. It is also unclear from section 46 of the PDPA whether the proposed fines will be imposed on the basis of (i) each

MICA's position in the Proposed Data Protection Act (PDPA)	Remarks / StarHub's further submission, if any
	terminated telephone number, or (ii) each batch of terminated telephone numbers. We submit that MICA should consider a grace period, given the complexities involved. Further, the financial penalty should only be imposed on a step up basis, wherein a higher penalty is imposed only where there are multiple failures.
The primary responsibility for ensuring that the lists of telephone numbers have been "filtered" as required by law lies with the organisation responsible for the product or service, even if the organisation authorises another organisation to send the specified messages. It would be up to the authorising organisation to take suitable messages to guard against any breach by any agents, partners or vendors it engages. (Paragraph 2.173)	We propose that MICA clarify the definition of "send" and "sender" in the PDPA. As it is currently defined to include the sending of the message, causing of the message to be sent, or authorisation of the sending of the message. It is not clear that the primary responsibility lies with the organisation responsible for the product or service. We propose that the definition of "send" and "sender" should expressly exclude parties who are acting as a conduit or agent on behalf of the party authorising the sending of the message e.g. where the function has been outsourced to a telecom service operator or specialised call centre.
Penalties will be capped at up to $10,000 per breach, and up to $1,000 in composition fines. Penalties will be imposed for the following breaches: (1) Sending message without checking with the DNC Registry within 30 days of sending the message; (2) Sending message without receiving confirmation that the telephone number is not listed in the register; (3) Sending message without identifiable originating number or sender name, or without contact information in message; and (4) Failure by telecommunications licensees to provide information on terminated numbers. (Paragraph 2.181)	We are of the view that the proposed financial penalties under the PDPA are too harsh and oppressive. The proposed penalties do not commensurate with the potential inconvenience experienced by a consumer who has received a marketing message despite being listed on the DNC Registry. We submit that MICA should consider a grace period, given the complexities involved. Further, the financial penalty should only be imposed on a step up basis, wherein a higher penalty is imposed only where there are multiple failures.
DPC will have the power to require the cooperation of telecommunication licensees in the investigation of whether an organisation had breached the rules under the DNC framework. (Paragraph 2.182)	It would be onerous to require telecommunication licensees to assist in tracing calls made to the complainant. This is in addition to the obligation to provide the list of terminated numbers to the DNC Registry, in the form and

MICA's position in the Proposed Data Protection Act (PDPA)	Remarks / StarHub's further submission, if any
	manner requested by the DNC Registry. As there are costs involved in extracting the information and tracing calls made to the complainant, such costs must be passed on to the DNC, given that consumers need not pay any charges to register themselves on to the DNC Registry. Also, it should be made clear that the provision of such information by the telecommunication licencees will not result in a breach of their obligations under the sectoral regulations.
MICA plans to implement the DNC Registry at least 12 months from the time the PDPA is enacted. (Paragraph 2.184)	We submit that the "sunrise" period should be 18 months. 1 year would be too short. Many organisations would still be adapting and ensuring compliance with the PDPA. The introduction of the DNC Registry would require organisations to expend further time, money and resources to modify their marketing and sales processes to achieve compliance with the DNC Registry.

3. CONCLUSION

StarHub welcomes the opportunity to provide feedback on the proposed Personal Data Protection Bill by the Ministry of Information, Communication and the Arts ("MICA") and supports the need for legislation to keep pace with developments in the industry and with market conditions.

The key areas of StarHub's response to the proposed Personal Data Protection Act ("PDPA") are as follows:

(i) The proposed PDPA should not apply concurrently with existing sectoral regulations, failing which there could be uncertainty and confusion. Instead, we submit that where the industry is subject to sectoral regulations, these should take precedence over the proposed PDPA.

(ii) It would not be practicable to restrict the consent obtained from an individual only to what is necessary to provide the product or service. This approach is unduly narrow and restrictive. Instead, the touchstone should be a reasonably scoped consent.

(iii) An "opt-in" approach would be onerous and impractical, especially in the case of organisations which already have a large consumer base. Instead, we propose that where organisations are subject to sectoral regulations which currently provide for an "opt-out" approach, this should take precedence over the proposed PDPA.

(iv) It would not be practicable to require organisations to keep track of the duration in which personal data has been used and the ways in which personal data has been used, especially for organisations which have a large consumer base. Instead, we propose that it would be sufficient for organisations to abide by its internal retention policies. During the period of retention, the organisation would be bound by the proposed PDPA and/or sectoral regulations.

(v) The proposed penalty and enforcement regime under the PDPA is too harsh. Instead, we propose that financial penalties should only be imposed on a step-up basis, wherein a harsher penalty is imposed only in instances of repeated violations by organisations.

(vi) As regards the proposed National Do-Not-Call ("DNC") Registry, telecommunication licensees should not be required to provide the list of terminated numbers to the DNC registry on a monthly basis. The costs of requiring telecommunication licensees to comply with this requirement are likely to outweigh the costs of adopting an alternative approach i.e. to allow individuals to make enquiries on the status of their own phone numbers, for free or at a nominal charge. Further, the proposed penalty on telecommunication licensees for failure to provide the list of termination numbers is too harsh.

(vii) The proposed penalty and enforcement regime is too harsh and does not commensurate with the potential inconvenience experienced by a consumer who has received a marketing message despite being listed on the registry. Instead, we propose that financial penalties should only be imposed on a step-up basis, wherein a harsher penalty is imposed only in instances of repeated violations by organisations.

StarHub is grateful for the opportunity to comment on this matter.

StarHub Ltd
30 April 2012