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

PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE

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

25 October 2011

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

1. EXECUTIVE SUMMARY

StarHub welcomes the opportunity to provide feedback on the proposed consumer data protection regime 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 proposed consumer data protection regime plays an important role in establishing safeguards to protect consumers' personal data and in promoting greater consumer trust in the private sector.

The key areas of StarHub's response to the proposed consumer data protection regime are as follows:

(i) The proposed data protection regime should not apply concurrently with existing sectoral regulations. Instead, we submit that where the industry is subject to sectoral regulations, these should take precedence over the proposed data protection regime.

(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 restrictive.

(iii) An "opt-in" approach would be onerous and impractical, especially in the case of organizations which have a large consumer base. Instead, an "opt-out" approach should be adopted.

(iv) The requirement on organisations to assist an individual in obtaining access to his personal data and provide the individual with detailed information about the ways in which his personal data has been used is impractical and onerous. We submit that there are sufficient safeguards in sectoral regulations and the proposed data protection regime.

(v) The proposed data protection regime should be of prospective effect and should not affect data collected before the proposed data protection legislation comes into force.

(vi) We are supportive of the proposition to establish a national Do-Not-Call Registry. However, we have some concerns in relation to how the Do-Not-Call Registry will be implemented. In particular, we submit that the cost of the Registry should be borne by the telemarketing industry.

StarHub is pleased to provide its comments on the proposed data protection regime in the following section.

2. COMMENTS

	Recommendations by MICA	Reference	Comments
1.	Application with sectoral regulations Proposed data protection regime will apply a general baseline concurrently with existing sectoral regulations, which could impose more stringent data protection standards where necessary.	Paragraph 3.8	It is important for there to be certainty, to facilitate compliance. As such, the data protection regime should not apply 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. Instead, we submit that where organisations are subject to existing sectoral regulations, such sectoral regulations should apply. The data protection regime should be similar to the competition law regime, which adopts the approach that the provisions of the Competition Act shall not apply where another regulatory authority has jurisdiction (e.g. in the aviation industry and the postal service industry). This approach would also tap on the specialised knowledge of the sectoral regulator and allow it to regulate the industry it is familiar with, in place of a generic regulator. If this approach is not taken, conflicts and discrepancies could well develop between the sectoral regulations and the data protection regime. An organisation could find that, in complying with one set of regulations, it is in breach of the other set. To avoid this scenario, it is essential for organisations to only be subject to one set of regulations, and we propose that sectoral regulations should take precedence.
2.	Personal Data of Deceased Individuals MICA has sought views on whether the personal data of deceased individuals should be covered by the proposed data protection law. In the event that such data is to be included, one possible approach is to accord the same level of protection to the personal data of deceased individuals as that of living individuals, only in relation to	Paragraph 3.16	We submit that it would be impractical for the proposed data protection law to apply to deceased individuals. In such a situation, it would be an onerous requirement on organisations to, *inter alia*: (i) identify and verify whether a living relative is able to act on behalf of the deceased;

	Recommendations by MICA	Reference	Comments
	the safeguarding and disclosure of such personal data, and where the individual has been deceased for less than 20 years.		(ii) arbitrate in the event where there is a dispute as to who should be acting on behalf of the deceased; and (iii) determine whether a living relative has agreed to act on behalf of the deceased in granting consent as regards the personal data of the deceased.
3.	Scope of Consent An organisation may not, as a condition for supplying a product or service, require an individual to consent to the collection, use or disclosure of personal data beyond what is necessary to provide the product or service.	Paragraph 3.31	We submit that it would not be practical to restrict the consent to the collection, use or disclosure of personal data to what is necessary to provide the product or service. This approach is unduly restrictive and is likely to restrict the options open to consumers, given that new products and services are always evolving. We would suggest that it would be more practicable to adopt the approach taken under the IDA Telecom Competition Code and MDA Competition Code, which provide general restrictions on the use of personal data unless authorisation has been given by the consumer. This approach would allow organisations to collect personal data and seek consent from consumers for broader purposes, and the data protection regime would apply general restrictions as to how the organisation may use the personal data collected e.g. restrictions on the use for the development or marketing of other goods or services and restrictions on disclosure to any third party.
4.	"Opt-Out" Approach for obtaining consent Some jurisdictions deem consent to be given when individuals are notified of an organisation's intent to collect, use or disclose their personal data, but do not register any objections within a reasonable timeframe. While such an "opt-out" approach may be more cost effective for organisations, MICA notes that it may be unreasonable to place the burden of establishing consent on the individuals. MICA would like to seek views on whether the Data Protection Act should also deem consent to be given in such situations.	Paragraph 3.35	We submit that it would be onerous and impractical for organisations with a large customer base to have to contact each individual for express consent. By way of example, for a large organisation such as Singapore Power, it would be extremely costly and time-consuming for them to have to contact almost every household in Singapore for express consent. This obligation would be particularly burdensome on those organisations which are already subject to sectoral regulations, which operate on an "opt-out" basis. Further, an "opt-out" approach would be consistent with the Singapore culture, where the "opt-in" rate is likely to be low. We

	Recommendations by MICA	Reference	Comments
			note that this culture has been recognised by the Singapore government as well in the implementation of the "opt-out" regime under the Human Organ Transplants Act. An "opt-out" approach should similarly be adopted under the proposed data protection regime instead. We would however suggest that organisations be obligated to provide easy channels for consumers to "opt-out". This would address any concerns MICA may have on placing an unreasonable burden on individuals to establish consent.
5.	Protection of Personal Data The Data Protection Act will require organisations to protect personal data in its custody or under its control, by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or other similar risks. Specific methods of securing personal data will not be prescribed in the Data Protection Act, but guidelines may be issued on suitable methods of protection that can be considered by organisations.	Paragraph 3.64 and 3.65	We propose that MICA provide greater clarity as to the type of security arrangements which need to be adopted by organisations to protect personal data. On this note, we submit that the requirement for security arrangements should consider a balance between the requirement to protect personal data and the costs to be incurred by organisations in having to maintain such security arrangements and systems.
6.	Specifying Retention Period Whether organisations should be required to specify the retention period at the point of collecting the personal data.	Paragraph 3.67	We submit that it would be impractical and costly for organisations to specify the retention period at the point of collecting the personal data. This is especially so for organisations with a large consumer base, as retention periods would depend on individuals and the type of data collected. Further, the retention policies of organisations may evolve over time and it would not be practical to require organisations to specify the retention period upfront. For instance, retention policies may change depending on whether the records are physical or electronic, or whether the physical data has been transferred to an electronic medium.
7.	Access to and Correction of Personal Data Generally, upon request of an individual, the organisation	Paragraph 3.68	We submit that this requirement would be impractical and onerous. Further, we submit that there are already sufficient

	Recommendations by MICA	Reference	Comments
	should take steps to assist the individual in obtaining access to his personal data, provide the individual with information about the ways in which the personal data has been and is being used by the organisation, and provide the individual with the names of the individuals and organisations to whom the personal data has been disclosed.		safeguards in the proposed data protection legislation and sectoral regulations which govern the purposes for which personal data may be used. Accordingly, there is no need to over-regulate and require organisations to keep track of the ways in which personal data has been used and how it has been disclosed.
8.	Refusing Access to Personal Data The organisation may refuse individuals' access to their personal data where they face frivolous or vexatious requests, or where responding to the request would unreasonably interfere with the operations of the organisation due to the repetitious or systematic nature of the requests. This also applies if the information request is trivial, not readily retrievable, does not exist or cannot be found, or the burden or expense of responding to the request would be unreasonable or disproportionate to the risks to the interests of the individual who made the request.	Paragraph 3.73	We support MICA's position that the organisation should be given the discretion to refuse frivolous or vexatious requests for access. Such access should only have to be given where the individual is able to show that his request is reasonable and necessary. Further, the organisation should be allowed to charge a reasonable fee to recover costs incurred in providing such access.
9.	Penalty and Enforcement Regime It is proposed that the DPC will have powers to issue orders for an organisation to rectify non-compliance with the proposed data protection law, and require the organisation to pay, within a specified period, a financial penalty of such amount not exceeding $1 million. Given that the Data Protection Act is expected to operate concurrently with other sectoral regulations, there may also be cases where a particular incident may constitute a breach in both regimes. In such cases, it would be preferable that the organisation be subject to the investigative and enforcement actions of one regulator. The Data Protection Act will therefore provide the DPC with the powers to refer an incident to another regulatory agency if necessary.	Paragraph 4.4 Paragraph 4.9	We reiterate our submission that the data protection regime should not apply 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. Instead, we submit that where organisations are subject to existing sectoral regulations, the organisation should 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.

	Recommendations by MICA	Reference	Comments
10.	Penalties The proposed penalty regime recognises that the majority of contraventions would be minor or non-malicious in nature, and would be adequately addressed by the issuance of orders for corrective action. However, there could also be violations that would warrant stiffer penalties, such as those that cause significant harm to individuals. In such instances, financial penalties could be imposed on top of any orders for corrective action.	Paragraph 4.5	We submit that it is necessary for MICA to clarify the circumstances under which financial penalties will be imposed. We would suggest that financial penalties should only be imposed where: (i) there has been significant harm caused to individuals e.g. if the individual's safety is threatened; (ii) the organisation or individual has been errant and repeatedly non-compliant with the orders of the DPC; or (iii) the organisation or individual has knowingly or recklessly contravened the law, made false statements, misled the DPC or failed to comply with orders made by the DPC. In the absence of such clarity it is unclear to organisations when or if penalties might be imposed on them, creating unnecessary uncertainty.
11.	"Sunrise" Period MICA is considering a "sunrise" period between 1-2 years, and would like to seek public and industry feedback on the appropriate length of a sunrise period.	Paragraph 4.14	We submit that the "sunrise" period should be at least 2 years, as 1 year would be onerous. Many organisations may need to expend significant time, money and resources to modify their customer management systems to comply with the new regulations.
12.	Treatment of Existing Personal Data MICA's proposal is to deem that consent was already given by the individual concerned for the organisation to use and/or process existing personal data. This would however be restricted to reasonable existing uses, taking into account the nature of the organisation's business.	Paragraph 4.17	We agree with MICA's position. We submit that in adherence to the rule of law and the importance of ensuring certainty, the proposed data protection regime should be of prospective effect. This would also not affect accrued contractual rights prior to the implementation of the regime.
13.	National Do-Not-Call Registry MICA proposed to set up a national Do-Not-Call Registry, to provide the individual with a simple and effective way to opt-out of all telemarketing messages without having to		We are supportive of MICA's initiative to establish a national Do-Not-Call Registry. This will ensure that individuals are able to opt-out of unsolicited telemarketing calls, SMS and fax messages from organisations. However, we have concerns as to how it will

	Recommendations by MICA	Reference	Comments
	manually withdraw consent from every organisation for the purpose of telemarketing.		be practically implemented. We propose that MICA clarify the following: • Who will bear the costs of maintaining the Do-Not-Call Registry? • Who will bear the responsibility of maintaining the Do-Not-Call Registry? • In the situation where an organisation sends telemarketing messages on behalf of another organisation (e.g. where the marketing agency sends messages on behalf of a service provider), which party will be held responsible for ensuring that messages are not sent to individuals in the Registry? • How will the Registry's database be made available to organisations, to facilitate synchronisation with organisations' database? • How long will it take for a consumer's request to be reflected in the Registry's database? • How will organisations be notified of changes to the database? • How often will organisations be expected to update their database to synchronise with the Registry's database? In line with the principle of "cost-causality" we submit that the costs of establishing the Do-Not-Call Registry should be funded by the telemarketing industry. Such an outcome would be equitable and efficient, and in line with international precedent (as this is the approach the countries such as Australia have adopted). We would have strong concerns if the cost of the Do-Not-Call Registry were imposed on parties outside of the telemarketing industry.

3. CONCLUSION

StarHub welcomes the opportunity to provide feedback on the proposed consumer data protection regime 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 consumer data protection regime are as follows:

(vii) The proposed data protection regime should not apply concurrently with existing sectoral regulations. Instead, we submit that where the industry is subject to sectoral regulations, these should take precedence over the proposed data protection regime.

(viii) 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 restrictive.

(ix) An "opt-in" approach would be onerous and impractical, especially in the case of organizations which have a large consumer base. Instead, an "opt-out" approach should be adopted.

(x) The requirement on organisations to assist an individual in obtaining access to his personal data and provide the individual with detailed information about the ways in which his personal data has been used is impractical and onerous. We submit that there are sufficient safeguards in sectoral regulations and the proposed data protection regime.

(xi) The proposed data protection regime should be of prospective effect and should not affect data collected before the proposed data protection legislation comes into force.

(xii) We are supportive of the proposition to establish a national Do-Not-Call Registry. However, we have some concerns in relation to how the Do-Not-Call Registry will be implemented. In particular, we submit that the cost of the Registry should be borne by the telemarketing industry.

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

StarHub Ltd
25 October 2011