Answers to Questions contained in the
Singapore MICA Consultation Paper for Proposed DP Legislation

Provided by SPYRUS, Inc.

25 October 2011

Question#	Question Text	SPYRUS Answer
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?	**The proposed DP Law is specialized to protect the average citizen and does not address specific needs of diplomatic, military and financial communities. It is assumed that sensitive governmental and financial data is protected concomitantly by other laws.**
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?	**Cross-sector flows should be facilitated, as is the intension of the DP Law. This should be complemented by appropriate sectorial regulations where additional protection is required.**
3	Do you have any views / comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?	**The proposed definition could preclude use of an NRIC number as an identifier in banking and financial contexts. This should be examined.**
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	**There may be a need to examine this data with respect to damage to the deceased individual. As in other contexts, data relating to a deceased individual may be less sensitive to privacy concerns, but may still be open to exploitation in fraudulent attacks, such as use of personal identifiers in identity theft. As in some other jurisdictions,**

	it should, do you have any views / comments on the proposed approach to the protection of personal data of the deceased?	**the use of a "sunset" period, say 20 years, may prove adequate mitigation of risk.**
5	Do you have any views / comments on the proposed organisations covered by the DP law?	**The scope of the DP Law should remain the private sector and have a "light touch" approach as proposed. Too much stringency will act as a retardant to legitimate business and cause law-enforcement costs to rise without necessarily impeding criminal activities.**
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?	**Use of the UK model is recommended. Servers and cookies within the boundaries of Singapore is a realistic scope for the DP Law. External sites may evade prosecution and render the law unenforceable.**
7	Do you have any views / comments on the proposed general exclusions from the DP law?	**The exclusions are adequate. The DP Law should apply to targets of collection and/or retained information storage, use or disclosure within Singapore's boundaries.**
8	With reference to paragraph 3.26, do you have any views / comments as to whether there should be exclusions for artistic and literary purposes under the DP Act? How should these exclusions be defined if exclusions	**Although exclusions in Canadian privacy law are made for artistic / literary purposes, it is unclear that this exclusion would not be unduly exploited by criminal elements. It may be safer to exclude only on the basis of permission by the target of collection. See also question 11's answer.**

	for artistic and literary purposes should be provided for?	
9	Are there any other exclusions that should be catered for under the DP Act?	**Bona fide medical research or medical diagnostic services in a hospital could be a realistic exclusion deserving special provisions. Other areas of health data collection, such as health insurance or biometric data should be stringently protected.**
10	Do you have any views / comments on the proposed general rules under the DP law?	**The general rules are acceptable.**
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?	**The British Columbia PIPA law is reasonable, enforcing notification but allowing "opt-out" response by the citizen within a reasonable time-frame. It may be fairer to allow unlimited time-frame for opting out in cases where damage to the individual occurs at a later date.**
12	Do you have any views / comments on the proposed rules on collection, use and disclosure of personal data?	**Consent, purpose and reasonableness are main concerns in collection, use and disclosure of private information. Reasonableness is more open to interpretation than the others.**
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	**As in the Canadian Privacy Act there should be a provision for the right of an individual to request correction of erroneous collected information, or information that no longer applies to the individual. There is a need for an official role such as "privacy commissioner" who would audit the use and application of the DP Law and advise government of anomalies and violations, as well as taking responsibility to parliament for the application of the law.**

	the organisation? Are there any other exceptions that should be provided?	
14	Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined at paragraphs 3.60 to 3.61?	**The onus must be on the collecting / transferring organization to ensure protection of data both in transit and at rest in the destination country. The level of protection must be reasonably similar to what would be enforced in Singapore, ceterus paribus. See answer to question 9 for areas that may require stringent protection.**
14a	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?	**Enforced retention periods is a good idea, as is the right of the individual to review and apply for correction / removal of erroneous data. Safe destruction of stored information is a prerequisite to privacy. The problem of data remanence for information stored in ferromagnetic materials should be explicitly addressed. The problem of plaintext information as opposed to encrypted information storage is not dealt with in this text. The storage of cryptographic keys that result in the decryption of private information may need further definition. The level of assurance provided by individual cryptographic algorithms may need further definition.**
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?	**See answer to question 14a.**
16	Do you have any views / comments on the proposed rules on access to and correction of personal data?	**See answer to question 14a. The exemptions for legal privilege and commercial confidential information are reasonable. Frivolity and vexation with respect to personal data review are not well defined, and should be.**
17	Do you have any views /	**Enforcement and penalty should be in line with current practice**

	comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?	**regarding paper-based information in Singapore. A damage test to the individual should be relevant in prosecutions.**
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?	**In cases of extreme damage for disclosure, the penalty to the organization or individual collecting the private information should be an effective deterrent. Failure of an organization to use adequate computer security-enforcing technology and/or countermeasures should be equally punishable as well. Security audit including penetration tests and risk management procedures should be requirements for organizations collecting, storing, using or disclosing private information. Evidence of security audit should be available and reviewable to the appropriate governmental agency on demand.**
19	Do you have any suggestions on specific guidelines that the DPC should provide to help organisations achieve compliance with the DP law?	**See answer to question 18.**
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?	**The transitional plan is reasonable. A two-year period may be more appropriate for Singapore, especially if demands for more stringent security audit and risk-management practice are new requirements.**
21	With reference to paragraphs 4.15 to 4.19, do you have any views / comments on the proposed treatment of existing personal data?	**Some reasonable balance must be present in the DP law between compliance for new data vs. compliance with existing data. The principle given in 4.17 is reasonable. The after-enactment requirements of 4.18 are also reasonable. Perhaps the term "existing use" should be more carefully defined.**

22	Are there certain organisations that may require different transitional arrangements?	**The "lighter touch" should be applied to small business, in cases where costs may be prohibitive. Governmental institutions and large organizations should comply with a greater adherence to the law.**
23	Do you have any views / comments as to whether a National Do-Not-Call registry should be set up in Singapore?	**In some countries (e.g., Canada) studies (see: http://toronto.about.com/od/federalgovernment/ht/do_not_call.htm) have shown that not all participants are pleased with the results of the national no-call list. Some external organizations who can evade the provisions of the rules use the list as a mine for phone numbers to call, contrary to the intension of the list. Examination of how enforceable the law is regarding no-call protection should be done before amassing a data store highly valued by the intended perpetrators.**