Proposed Consumer Data Protection Regime for Singapore by MICA

A) In General:

Page 8:

3.16 Given the complexity of this issue, MICA would like to seek views on whether the personal data of deceased individuals should be covered by the proposed DP 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 the safeguarding and disclosure*** of such personal data, and where the individual has been deceased for less than 20 years. Such an arrangement will strike a balance between mitigating the impact of inadequate protection of the personal data of deceased individuals, which would be most pernicious in the event of ***disclosure without consent***, and minimising compliance costs for organisations.

>> In general, guidelines should be established to allow seeking consent on behalf of the person; especially for deceased person; existing data of non-contactable living person and who can request for the info & who can give consents.

Page 10:

3.22 However, while there are valid reasons for extending the coverage of Singapore‟s DP law to all data collection and processing activities in Singapore, regardless of whether the organisation responsible is in Singapore, there are practical difficulties to implementing such a regime. In particular, where the organisation in question has no presence in Singapore, it would be difficult to carry out investigations into any complaint made in relation to an activity of the organisation, or to proceed with any enforcement action against the organisation. In practical terms, even if such activities are to be included in Singapore‟s DP law, the limited ability to carry out investigation and enforcement may mean that consumer complaints against organisations outside of Singapore cannot be adequately addressed, and breaches by such organisations may remain uncorrected. MICA would like to seek views as to whether Singapore‟s DP law should ***only cover organisations in Singapore, or whether coverage should also extend to personal data collection and processing activities in Singapore regardless of where the organisation is located***, bearing in mind the practical difficulties of implementation.

>> In general, it should be regardless of where the organization is located. Guidelines should be established as many of the organizations today may not even be based in a single country.

Page 20:

3.60 While the proposed DP law will apply to organisations in Singapore, it is important for consumers ***to have the assurance*** that similar standards of protection are accorded to their personal data if the data is transferred outside Singapore. This is important to maintain the level of trust and confidence of consumers in Singapore, especially as cross-border data transfers become more commonplace with market developments like cloud-based computing.

3.61 Some jurisdictions like the EU impose stringent conditions on the transfer of EU data outside the EU. In particular, data may only be transferred to non-EU (or non-EEA25) jurisdictions that have been found to have an adequate level of data protection, or where companies have adopted specific measures such as approved binding corporate rules or

standard contractual clauses. Other jurisdictions impose alternative rules in relation to cross-border data transfers, such as APEC‟s proposed Cross-Border Privacy Rules system. For Singapore, the proposal is to adopt a “principle based” approach, as opposed to a more prescriptive approach of requiring adequacy rulings for foreign regimes or approving binding corporate rules. The onus will be on the organisation to ensure that appropriate measures are taken to protect personal data where such data is transferred outside Singapore, as the organisation is considered to have control over the data.

>> In general, how would the DP act apply to organisations outside Singapore which may not be under the governance of DP act.

Page 21:

3.67 Ideally, individuals should be informed of the retention period for their personal data at the point of collection, as this would provide greater assurance to individuals and encourage sharing of data. However, MICA recognises that the appropriate retention period may differ according to context, and it may not always be practicable for organisations to determine and specify a suitable retention period upfront. MICA would thus like to seek views on whether organisations should be required to specify the retention period at the point of collecting the personal data.

>> In general, it might be challenging to specify retention period at the point of collecting the personal data. There would also be a need to communicate changes if any to the clients.

Page 24:

4.4 It is important to highlight that the penalty regime proposed for Singapore’s DP Act seeks to secure ongoing compliance by organisations and at the same time, provide sufficient deterrence to ensure that organisations put in place appropriate measures to safeguard consumers’ personal data. The proposed penalty regime is thus a tiered one that will enable the DPC to enforce remedies commensurate with the seriousness of the violation. Specifically, it is proposed that the DPC will have powers to issue orders for an organisation to rectify non-compliance with the DP law, and require the organisation to pay, within a specified period, a financial penalty of such amount not exceeding $1 million. The financial penalty is notwithstanding any order already made by the DPC.

>> In general, how to impose penalty on overseas organisations that are governed by other jurisdictions?

Page 21:

3.66 Thirdly, it is important to strike the right balance between the need for organisations to retain personal data, where there are valid reasons to do so, and the requirement to delete personal data (or render such data anonymous such that the data is no longer personally identifiable). It is noted that organisations collect and use personal data for specific purposes, and where the data is no longer necessary to serve such purposes, organisations should not retain such personal data. To strike the balance, it is proposed that if an organisation uses an individual's personal data to make a decision that directly affects the individual, the organisation shall retain that information for a sufficient period of time after using it ***so that the individual has a reasonable opportunity to obtain access to it***. Following that, an organisation shall then destroy its documents containing personal data, or make such data anonymous, when retention is no longer necessary for legal or business purposes, and as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data.

>> How would this be applied practically in the healthcare sector? Patients are not given access to their own medical records currently, unless it's going to be opened up in future (with patient portal?).

Page 22:

3.68 It is proposed that individuals will have the right to request access to their personal data held by an organisation. This 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 DP Act. Generally, upon the request of an individual, the organisation 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***. Credit bureaus should also provide the individual with the names of the sources from which they received the personal data, unless it is reasonable to assume the individual can ascertain those sources.

>> How would this be applied practically in the healthcare sector? In general, it will be an operation challenge to provide info of names of individuals & organizations to whom the personal data has been disclosed.

Submitted by	: Lok Yoke Har/Emileen Chia
Organisation	: Institute of Mental Health
Contacts	: Yoke_Har_lok@imh.com.sg/Emileen_chia@imh.com.sg