Jointly by:

Name: Jamie Chong Mei Soon Company: ORIX Leasing Malaysia Berhad Department: Group Legal & Compliance Contact No.: +603-2632 7372 Email: JamieChong@orix.com.my	Name: Ong Chan Seng Company: ORIX Leasing Malaysia Berhad Department: Group Legal & Compliance Contact No.: +603-2632 7369 Email: OngChanSeng@orix.com.my

Statement of Interest:

ORIX Leasing Malaysia Berhad wholly owns ORIX (Rentec) Singapore Pte Ltd, our subsidiary in Singapore. We have an interest in the amendment of the PDPA 2012 as it will affect the operations of our subsidiary.

Comments:

Accountability principle

By making accountability explicit through the amendment of Part III of the PDPA (Clause 4 of the draft PDPA (Amendment) Bill), it adds more clarity in that organizations are under an obligation not only to protect personal data in their possession or under their control but they are accountable for it and must be able to comply with the requirements under the PDPA.

It is reasonable and expeditious steps to remedy breaches – unreasonable delay to notify the PDPC & affected individuals i.e. no later than 3 calendar days after determining breach meets notification criteria. While apparent data breach is inexcusable for delayed notification, there should be leeway for determining and notifying latent breaches.

Under exceptional circumstances where notification to affected individuals are not desirable, PDPC may exempt e.g. national security, compromise investigation. A Whitelist for types of a data breach requiring notification and for notification exemption eligibility would enable better illustration of the requirements.

In overall, this is definitely a recommended amendment to emphasize on organizations' accountability and demonstrate the importance of protecting personal data from misuse.

Mandatory data breach notification requirement

Since PDPC/MCI intends to further enhance organizations' accountability, it is a good move to introduce a mandatory data breach requirement (Clause 12 of the draft PDPA (Amendment) Bill) as a central part of the accountability principle.

However, it is crucial for PDPC to spell out clearly what constitutes significant harm, the criteria which render the data breach notifiable, what amounts to the assessment of the data breach "in a reasonable and expeditious manner", the procedures to be complied with in notifying both PDPC and the affected individual and the exemptions to this requirement when a notification is impractical under certain circumstances.

In implementing this new requirement, PDPC needs to consider that the effectiveness of this requirement in protecting individuals also depends hugely on the effectiveness of the internal control, monitoring and reporting system of an organization. Organizations might need to incur high cost to put in place a proper control and monitoring system and this may not be viable for small-sized organizations.

Removal of exclusion for organizations acting on behalf of public agencies

The removal of this exclusion (Clause 3(a) of the draft PDPA (Amendment) Bill) is recommended unless there is any good reason for such exemption. There should be no double standards when it comes to protection and accountability for personal data.

Offences relating to egregious mishandling of personal data
Strengthening of organizational accountability will only be possible and meaningful if individuals who handle or have access to personal data are also subject to an accountability obligation. Therefore, the introduction of the new offences is a good way to enforce accountability at the individual level.

Enhanced framework for collection, use and disclosure of personal data
Deemed consent by contractual necessity is necessary to enable the smooth performance of a contract or transaction. However, third party organizations must be limited to only those relevant to the conclusion or performance of a contract between an individual and an organization and these party organizations should have proper internal control, monitoring and compliance system in place.

Deemed consent by notification is an amendment that would generally be welcomed by organizations. However, what amounts to appropriate notification? If proper notice is sent to the individual but not received by him or her and therefore, he or she is not able to opt-out, then there should no consent deemed given.

And if deemed consent is also implied consent, it would appear contrary to the GDPR that consent is freely given, specific, informed and unambiguous and the need for implied consent to be properly recorded and maintained by data user for it to be acceptable.

The two new exceptions to the consent requirement i.e. legitimate interests exception and business improvement exception are welcomed as the necessity of collection, use or disclosure of personal data outweighs the adverse impact of the individual but these exceptions should only apply in very limited and narrow circumstances.

Data Portability Organization
The new data portability obligation should be a welcome move because it benefits not only individual consumers by allowing them to switch service providers more easily but also promotes healthy competition among businesses. The question is how organizations ensure that the individual's personal data is securely transmitted to another organization? Higher cost and expenses might be involved to implement internal and monitoring system and a better IT security system and measures to prevent data leakage.

Improved controls for unsolicited commercial messages
Amendment of the SCA should cover messages sent to IM accounts via all sorts of platforms to accord adequate protection to individuals from being harassed by unwanted messages from organizations. The burden should be on organizations to find better ways to market their products and services and to maintain a business relationship with their customers.

Furthermore, the proposed incorporation of the Personal Data Protection (Exemption from Section 43) Order 2013 into the DNC provisions will still enable businesses to keep in touch with their existing customers.

Introduction of obligation and liability on third-party checkers is highly recommended since some organizations do rely solely on them to do the checking and there is no good reason why these third-party checkers should not be held accountable.

Enforcement of DNC Provisions under administrative regime
Organizations with adequate personal data protection regime in place should welcome the proposed measures to effective enforcement of the DNC.

While this will enable PDPC to resolve DNC complaints more efficiently and proportionately, will this change affect the level of compliance by organizations?

Require attendance
This is a good move to ease investigation by PDPC.

Statutory undertakings
This appears to be a good move to strengthen organizational accountability but what about those organizations without a proper data protection management plan in place? To implement one may result in huge financial constraint on these organizations.

Prohibitions to providing access
The reduction of the scope of prohibitions in this area is definitely recommended to minimize implementation issues for organizations providing access to personal data.

Conclusion:
The proposed amendments are generally welcomed with certain issues needed to be considered in terms of the difficulty level faced by organizations in implementing the same.