Cover Page

Particulars of organizations and contact person

Submitted by:
Mr. Lim Kian Kim

Lim Kian Kim is currently President of Singapore Cloud Forum (SCF) (www.cloud.org.sg) and Secretary of the Association of Information Security Professionals (AiSP) www.aisp.sg
This submission is in his personal capacity.

Summary of Major Points

1. An audit-based regime to protect individuals' personal data would reinforce our serious intention to be a trusted business hub in line with countries with data privacy or protection regimes. (Paragraph 3.15).

2. To reduce compliance costs associated with an audit – based regime, only organizations of certain revenue sizes should be subjected to audit. A potential guideline to adopt is the current one used by Accounting & Corporate Regulatory Authority for financial audit of companies. Using the same guideline would align the proposed DP framework to the overall regulatory efforts to promote Singapore as a business hub. (Paragraph 3.15).

3. Under the proposed definition of personal data, it presupposes a unique identifier before protection is conferred on the data. If the intent is to protect the information concerning or about a person, would "personal information" rather than personal data be more appropriate as a definition? (Paragraph 3.11).

4. A corporation may hold large quantities of disparate data but is either unable or does not need to identify the person associated with the data yet. Therefore the definition of personal data should include the phrase "information that may potentially or reasonably identify" a person. If not, any organization holding large amount of disparate data may be unduly affected. (Paragraph 3.12).

5. Exemption of sensitive personal from the proposed DP framework may have the effect of "watering down" the protection of data. Future exemption guidelines should be exposed to public feedback and review before implementation. (Paragraph 3.14).

6. As Government and government related entities do collect large quantities of data, exempting them would create an uneven approach in the way we manage data governance as a whole. Exempting the public sector without a similar regime may pose problems for cross recognition by countries with similar data privacy or protection regimes. This may then defeat the reason for creating the DP framework in the first place – to position Singapore as a trusted hub for business. (Paragraph 3.18).

7. The proposed DP framework should be extended to organizations outside of Singapore as long as the data is "Singapore related". The

Computer Misuse Act CAP (50) (A) took a similar position. Just like computer related crimes, identity theft and similar digital crimes are cross–border in nature. (Paragraph 3.20).

8. An "opt-out" approach while being cost effective for organizations, places an unreasonable demand on the individual. It must be remembered that the data belongs to the individual in the first place. (Paragraph 3.35).

9. The requirement and provision of a person within an organisation responsible for managing data signals the seriousness of the intent of the proposed DP framework. This should be a stand-alone position within the organization. Furthermore, the position should not be outsourced to a third party. The proposed DPC should also set up a framework to fund and train organizations planning for such a role as part of the roll-out plan for the framework during the "sunrise" period. (Paragraph 3.38).

10. Employers should provide a "basket of consent" so that the employee's data can be reused without seeking fresh consent to reduce cost. (Paragraph 3.45).

11. Exemptions to disclosure without consent should be severely limited unless there is a clear and present danger to the individual or it will defeat the purpose of the DP framework in the first place. This is especially so for data analytics as the ultimate objective of an analytics exercise is marketing or marketing related. It is fair that collecting agency should bear the cost of fresh consent for this purpose. Collecting organizations should include a storage and destruction policy. Destruction of collected data should be carried out within 12 months from the data of collection. (Paragraphs 3.54 to 3.59).

12. To avoid any ambiguity of how data would be treated, alternative methods of protecting data such as corporate binding rules should be subjected to review and approval by the proposed DPC before implementation. DPC should also list all approved corporations on their web site. Corporations should allow individuals to access and correct erroneous data collected in the first place as a principle of fairness, without placing unfair financial or bureaucratic barriers on such requests. Without being prescriptive, DPC may want to require that the methods used by corporations to protect data should at least comply with one of the many global standards on data security. (Paragraphs 3.60 to 3.61).

13. As a matter of balance, not more than SGD 5 is suggested if a cost is to be imposed on the individuals after the initial request to correct and or access data concerning the individuals. (Paragraphs 3.68 to 3.73).

14. A sunrise period of two years should be sufficient for affected organizations to comply with the proposed DP framework. The formation of a national Do-Not-Call Registry as part of the mechanism for protecting the data of individuals is a timely effort. (Part IV & V).

15. MICA should be commended for proposing a data protection framework as the current Model Code is clearly ineffective in today's context for data protection.

Comments

Questions in relation to objectives and principles of proposed DP framework
Question 1
Reference to paragraph 2.10
Comments

1. If the objective to implement a DP framework is to facilitate the cross border flow of data so as to position Singapore as a trusted business hub, an immediate question to consider is whether the thrust of the DP and the protection offered meets the so-called "adequacy" requirement of other similar data privacy / protection regimes. A regime that is too lax in terms of regulating the privacy of personal data is no different from a self regulatory model that has been found wanting in many aspects. It is suggested that the proposed DP regime should take an audit-based approach to ensure that organisations comply with the regime. Consumers are also assured that the protection of their data is taken seriously by the organizations as they are subject to audit on a regular basis.

2. To reduce the compliance cost, only organizations of certain size or revenue turnover is required to show that they are in compliance with regime. The Accounting & Corporate Regulatory Authority (ACRA)[1] , exempts companies of certain sizes from audit. Perhaps we should consider harmonizing with ACRA in determining which companies should be subject to a DP's audit.

Question 2
Reference to paragraph 3.8
Comments

1. The proposed DP framework is supposed to be a baseline regime applied concurrently with current sectoral regulations. This is on the assumption that the sectoral regulation is stricter than the DP framework.

2. If a sectoral regulation whether in whole or in part is less strict than the proposed regime, would the DP then mandate that that particular section be invalidated?

[1] Exempt Private Companies (EPC) with revenue not more than S$5 million for the financial year starting on or after 1 June 2004; or EPC with revenue not more than S$2.5 million for the financial year starting on or after 15 May 2003 but before 1 June 2004; or Any company, including an EPC, that is dormant for the financial year starting on or after 15 May 2003

Questions in relation to the definition of "personal data"
Question 3
Reference to paragraphs 3.9 to 3.11
Comments

Concern about definition being "unique identifier driven"

1. The current definition as it stands requires a unique identifier of a person such as his NRIC number before protection is conferred on the individual. If the intention is to protect the information of a person, should the definition be changed to "personal information" instead of "personal data"?

2. Does it mean that only information that is able to identify a person is relevant? This approach is fairly restrictive. For example, we may not know the name of our neighbour but we can definitely identify and know that he or she is living in the neighbourhood.[2] Information that may not identify a person but describes the person in sufficient details is "identifiable information".

3. Current web technology is able to collect seemingly innocent information that may not be linked to an identifiable individual for the moment, but if combined at a later stage with another piece of information such as the email address, would then clearly identified the person. Similarly a town CCTV may simple record certain characteristic of persons visiting the town, but if combined with information at a finer level, would then start to build up the profile of a specific individual.

Potentially or reasonably identifiable as a qualifier [3]

4. It is also important to qualify that holding information about an identified or identifiable individual is insufficient. The information should of such a nature that it may "reasonably" identify the person. This qualifier is important to large corporations that may hold large quantities of disparate data and yet at that stage have decided to use

---

[2] United Kingdom Government Information Commissioner's Office, *Data Protection Technical Guidance: Determining What is Personal Data* (2007), as quoted in *For Your Information Australian Privacy Law & Practice,* Australian Law Reform Commission,(2008) p300

[3] The Information Privacy Bill 2007 (WA) defines personal information, in part, as follows:
Personal information is information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead—
(a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or
(b) who can be identified by reference to an identifier or an identifying particular such as a fingerprint, retina print or body sample. Supra Note 2 p299

it to identify any person. For example, a public transport operator would possess large quantities of information about people using their system, and yet has no intention to identify the individuals. Without this qualifier, these organizations would need to incur costs to protect the information as "personal data" as it is currently defined.

5. The DPC in formulating the guidelines (Paragraph 3.12) should spell out the attributes of standalone information that if linked with other data or information may identify the individual. For example Internet protocol addresses if combined with usage patterns and other information such as email addresses would likely be able to identify a person.

Paragraph 3:14 Sensitive Personal Data: Minimum Criteria & Exemption Guidelines
Comments

6. Sensitive information is defined to include certain attributes.[4] By creating exemptions from the proposed DP regime, would it have the effect of "watering down" the protection given under the proposed DP framework? Would the exemption guidelines be open to public feedback and review?

Question 4
Reference to paragraphs 3.15 to3.16
No Comments

Questions in relation to the organisations and activities covered by the DP
Question 5
Reference to paragraph 3.18
Comments

<u>Exemptions of the public sector: Consistency, harmonization and governance</u>

1. As it stands, the proposed DP is the "baseline" law for protecting data. If the public sector which is a very large sector is exempted, how do we then ensure consistency by both public and private sector in treating the protection of data? Bearing in mind that government and government related bodies do collect huge amount of personal data, exempting them may create an uneven approach in how data should be protected, granted that there are current regulations within each

[4] 'Sensitive information' is defined in s 6(1) of the *Privacy Act* to mean information or an opinion about an individual's: racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal record. Supra Note 2 p 736

body on handling and protecting personal data. Should the public sector at least be required to comply with the principles of the proposed DP if there is no separate regime to regulate them, barring certain activities of the Government such as law enforcement and intelligence services?

2. Would the proposed DPC consider promulgating a series of broad level principles for mandatory compliance by government and related agencies? This position would also be in line with many international regimes where certain sectors of the Government are exempted due to the nature of the job where secrecy is needed to be effective.

<u>Exemptions of the public sector: Potential cross border recognition of privacy laws by other countries</u>

3. Commencing with Malaysia, it may be that the approach of Asian governments is to exempt the public sectors from the application of the data protection/privacy laws. However this would potentially create a situation where other regimes with similar but separate regimes to regulate their public sectors may not recognise the proposed DP as "adequate nor sufficient" to protect data of their citizens and therefore puts us in a less than desired hub for business and data management center.

Questions in relation to extending DP law to organisations located outside of Singapore
Question 6
Reference to paragraphs 3.20 to 3.22
Comments

The proposed DP law should be extended to organizations located outside of Singapore as long as they collect or process data related to Singaporeans and Singapore for the following reasons:

1. This is to ensure that organisations would not take advantage of this loophole to process Singapore related data without complying with the Act;
2. Organizations taking advantage of this loophole may not be legitimate business organizations and therefore we should include such potential organizations to deter potential criminal activities such as identity thefts;
3. Countries with data protection or privacy laws would consider the lack of potential recourse as another reason why our proposed DP framework is insufficient to meet the "adequacy" criteria of their similar regimes as their citizens' data, if processed together with ours are not protected; and

4. The ability to prosecute the organizations located outside Singapore is not new. The Computer Misuse Act (CAP 50) (A) provides prosecution against potential hacking activities conducted against a system, data or program located in Singapore whilst the perpetrator is outside Singapore. Identify theft like hacking is an activity that cuts across international borders. [5]

Question 7, 8 and 9
No comment

Questions in relation to the general exclusions from the DP law.
Question 10
No comment

Question 11
Reference to paragraphs 3.35
Comments

"Opt-out" Approach

1. An "opt-out" approach while being cost effective for organizations places an unreasonable demand and burden on the individual. It must be remembered that the data belongs to the individual and the organization seeking to benefit from the usage or collection of the data bears the necessary cost to obtain it. An opt-out approach presupposes that the individual data and its usages belong to the collecting organization unless the individual opts out.

Reference to paragraph 3.38
Comments

Accountability

The provision of a person within the organization to act as a liaison between the organization and their customers reinforces the importance of managing the data of their customers. To strengthen this role, the DP should prescribe the following criteria for such a role:

1. The role should be separate from other roles within the company. This is to ensure that the person has sufficient time and resources within the company to manage this function;
2. The person should have sufficient authority within the company to respond to queries from the DPC and customers without undue delay. Failure or undue delay to respond to a customer's query should be a cause of concern and investigation for the DPC;

[5] (3) For the purposes of this section, this Act shall apply if, for the offence in question — (*a*) the accused was in Singapore at the material time; or (*b*) the computer, program or data was in Singapore at the material time. CAP 50(A) s.11 (3)

3. The role should not be outsourced as a service to an external party such as accountancy or audit service as the person needs to be a full time employee of the organization to be able to respond any query effectively; and
4. DPC should provide training subsidies for companies during the sunrise period to prepare the companies for the implementation of the framework.

Questions in relation to the proposed rules on collection, use and disclosure of personal data.
Question 12
Reference to paragraph 3.45
Comments

Employee Personal Data

1. The purpose of collection of the employee's data is different from the original purpose in the first place. It is suggested that to reduce the cost in seeking consent, the organization should include a "basket of consent" that the employee agree to in the first place with the option to opt out if he or she is not agreeable for that data to be used later for another purpose different from at the point of collection.

2. Another issue is the employee's relative's data, such as those relating to their spouses and children. They should be included in the "basket of consent" with the ability to opt out for such usages as the DP framework suggested.

Question 13
Use/Processing
Reference to paragraph 3.49
No comment

Disclosure
Reference to paragraphs 3.51 to 3.53
No comment.

Reference to paragraphs 3.54 to 3.59
Comments

Disclosure to prescribed institutions

1. In general, the assumption is that these collecting agencies would include both government related agencies such as National Archives, health research organizations and private agencies.

2. Conditions of use, including purpose of collection should be stated upfront at the point of collection.

Disclosure without consent exception: Public Interest

3. Disclosure without consent would largely destroy the purpose of the protection of the data in the first place. The public interest should be clearly indicated to the user, if the data is to be disclosed without consent, without any punitive measure/s being imposed if consent is withheld by the data owner.

Disclosure without consent exception: Research

4. Similarly the definition of "research" should be clearly spelt out if disclosure is necessary without consent. The reason for collecting data for analytics is usually with the ultimate aim of using the data for marketing related activities, although exceptions are not inconceivable. Therefore it is reasonable for the collecting agency or body to bear the onus and or cost for informing the data owner for this purpose.

Disclosure without consent exception: Merger or acquisition

5. To protect the transfer of personal data, the DP framework should mandate that the personal data should be destroyed three (3) months from the date of failure to merge or to acquire, and a further requirement that the data cannot be used within the three months for marketing activities or to be transferred to another entity without fresh consent.

General Requirement Needed: Storage Period and Destruction Policy

6. Another key important policy that should be included is the storage and destruction policy. The collecting agency should state how long they intend to keep the data and what is the specific procedure they will use to destroy the data. It is suggested that by default, the data would be destroyed within 12 (twelve) months, and if kept further, fresh consent should be required.

7. The collecting agency should also state whether the data would be used in collaboration with another agency/private body in the pre-collection procedure with the ability to opt-out if necessary.

Question 14
Reference to paragraphs 3.60 to 3.61
Comments

1. To avoid any ambiguity on how the data would be treated, DPC may want to consider the following:

i. For companies using binding corporate rules, these companies should submit their rules to the proposed DPC for approval prior to transferring the data;
ii. The proposed DPC website should also list all approved companies under this category;
iii. In line with the principle based approach of this proposed regime,, DPC should formulate a set of policies for transfer of data and the onus is on the company to satisfy DPC that the necessary procedures and policies are in place to protect the date.

Proposed rules on accuracy, protection and retention of personal data
Question 15 (Re-numbered)
Paragraphs 3.62 to 3.67
Comments

Data Affecting an Individual: Accuracy –Correction Procedure

1. It is important for an individual to be able to challenge the accuracy of the data collected on that individual **IF** the decision would affect the individual based on erroneous data collected as a matter of fairness.

2. If a decision is made based on an erroneous data, the individual should be able to correct the error without unnecessary burden or cost.

3. Organization must put in place such correction policies and procedures and expose these procedures to the public, so that their customers are familiar of the processes they can use to seek re-dress.

4. The proposed DPC should also require the correction of erroneous data within a reasonable time frame by the organization, failing which the organization should be subject to punitive measures.

5. In addition, the individual should have recourse to reasonable compensation based on the failure of the company to correct the erroneous information if the failure impacted the individual financially as such.

Data Affecting an Individual: Security

6. Although the DPC may not want to be prescriptive in determining the method/s to secure the data, it may want to provide that the method used by the organization should comply with any one of the global

security standard used to protect such data. [6] DPC can then prescribe a list of standards the organization needs to comply with in handling the data of the individual.

Data Affecting an Individual: Retention Period

7. The recommended retention period should be reasonable to both the collection organization as well as the affected individual. To avoid being prescriptive, the collecting organization should not keep any data for more than 12 months as a matter of general practice from the point of collection, and fresh consent should be required, should there be a need to keep the data beyond 12 months.

Proposed rules on access to and correction of personal data.
Question 16 (Re-numbered)
Reference to paragraphs 3.68 to 3.73
Comments

Access and Correction of Personal Data: Cost

1. If an erroneous data is recorded or collected in the first place, the organization should provide access to correct for free. Otherwise we would be imposing punitive measures on the individual for the correction.

2. Subsequent fees impose on access and correction of personal data should be reasonable, and should not be used by collecting organizations as a source of revenue. The range should not be more than SGD5 per request as charged by the collecting agency.

Access and Correction of Personal Data: Refusal to Provide Access on Certain Grounds

3. Organizations should list the ground/s for denying access to and for correction of an individual's data. Such ground/s should be clear and explicit. Just as an individual should not request for access to correct data frivolously, the same treatment should be accorded to the individual.

4. DPC should provide an avenue for recourse for the affected individual through mediums as mediation.

Part IV: Implementation
A. Penalty and Enforcement Regime

[6] Standards for Security Categorization of Federal Information and Information Systems http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf, National Institute of Standards and Technology (NIST) (Computer Security Division), US.

No comment.

B. Regulations, Codes of Practice and Guidelines
Comment

1. The sunrise period should be at least for two years for the affected organizations to comply with the proposed DP framework.

Part V: National Do Not Call Registry
Comment
The set-up of a national Do-Not-Call Registry as part of the mechanism to protect the data of individuals is a timely effort.

Conclusion

1. MICA should be commended for proposing a DP framework for individuals as the Model Code is clearly ineffective in today's context for managing the protection of personal data.

2. Any framework for managing personal data is constantly a "work in progress" as technology continues to challenge us both in the ways we provide personal data and in how the collecting organizations manage them.