

**Submission to the Public Consultation on the Proposed
Consumer Data Protection Regime for Singapore**

By

**Professor Abu Bakar Munir
Faculty of Law, University of Malaya,
Malaysia**

13 October 2011

A. Question 3: Do you have any views/comments on the proposed definition of personal data outlined at paragraphs 3.9 – 3.11?

Paragraph 3.9 defines “personal data” to mean information about an identified or identifiable individual; where “individual” means a natural person, whether living or deceased.

Under this definition, the determining factor whether or not any information is personal data would depend on whether the data can identify someone or make someone be identified. In other words, the test to be used is whether or not the information could lead to an identification of a person. However, this is not clearly reflected in the given definition. Furthermore, the use of the word “about” in the definition makes the definition rather weak. There are many examples of records which will clearly be personal data where the information in question is not ‘about’ an individual but is about the activities which relate to them. For example, data such as personal bank statements or itemized telephone bills. These are personal data about the individuals operating the account or contracting for telephone services. For that matter, the information on “Miss Universe 2010” or “the winners of the Singapore General Election 2011” or “Nobel Prize Winners 2011” are all about the activities.

Another example, data about the salary for a particular job may not, by itself, be personal data. This data may be included in the advertisement for the job and will not, in those circumstances, be personal data. However, where the same salary details are linked to a name (for example, when the vacancy has been filled and there is a single named individual in post), the salary information about the job will be personal data ‘relating to’ the employee in post. In this scenario, the information about the salary is not in itself personal data but it becomes personal data where it can be linked to an individual to provide particular information about that individual.

Therefore, it is suggested that the word “about” is to be substituted by the words “which relates to” and “personal data” is to be defined in the following manner “any information which relates to an identified or identifiable natural person...”

All forms of personal data

The DP law, according to paragraph 13, will cover all forms of personal data, including both electronic and non-electronic forms of personal data. This will make the scope of the DP law too broad to cover even the processing of personal data by small traders and businesses as well as hawkers selling nasi lemak, roti chanai, etc, if they keep their customers data, for examples on papers or in their mobile phones. Perhaps, this may not be the intention of the DP law. The DP law should limit its application to personal data processed in electronic form and/or data processed **manually only if the data is so structured**. To achieve this, the DP Act may need to incorporate the concept of “relevant filing system” into it. Otherwise, as mentioned earlier, everyone including street hawkers will be subjected to the DP law.

“Relevant filing system” means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

In simple words, relevant filing system refers to information kept in a non-computerized manual system but sufficiently structured to allow easy access to information specific to the individuals. There are four criteria in deciding what constitutes a relevant filing system: (i) the personal data must be part of a set; (ii) the set must be structured; (iii) the data must be accessible; (iv) such access cannot be simply random but must be according to specific criteria. The overall effect of incorporating this concept is to restrict the scope of the proposed DP law. If any one of the four criteria is not met, the manually processed data concerned would not be covered. So, the processing of personal data manually will not be subjected to the DP law if the data is unstructured.

B. Question 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 it should, do you have any views/comments on how the proposed approach to the protection of personal data of the deceased?

Although a deceased person may ‘feel no shame or humiliation,’ there are sound public policy reasons for the proposed DP law to cover personal data of deceased individuals. However, since the DP law aims at protecting consumers’ data, the important question to be considered is, who is a “consumer”, and secondly, whether one can still be considered as a “consumer” if he or she has passed away.

The “consumer” is the one who consumes goods and services. The Supreme Court of India, in its landmark decision, *Lucknow Development Authority v. M.K. Gupta, (III (1993) CPJ 7 (SC))*, has held, that “the word ‘consumer’ is a comprehensive expression. It extends from a person who buys any commodity to consume either as eatable or otherwise from a shop, business house, corporation, store, fair price shop to use of private or public services.”

In Singapore, under the Consumer Protection (Fair Trading) Act 2003, “consumer” is defined to mean an individual who, otherwise than exclusively in the course of business — receives or has the right to receive goods or services from a supplier; or has a legal obligation to pay a supplier for goods or services that have been or are to be supplied to another individual. From this definition, arguably, the individual concern will have to be a living individual. Practically speaking, only a living individual can receive or has the right to receive goods or services from a supplier. The notion of “consumer” and the definition of consumer is often restricted to living persons.

The Consultation Paper in paragraph 3.6 states that the proposed DP law will be consistent with international standards provided for in OECD Guidelines and APEC Privacy Framework. The DP law will also make reference to data protection laws of other jurisdictions such as the EU, UK, Hong Kong etc. These international instruments do not cover personal data of deceased individuals.

If the DP Act is to cover deceased individuals, simply by defining “personal data” to include personal data of deceased individuals would be problematic. This is because of the fact that many of the data protection principles could not apply at all, or could apply only in part, to such data. For example, as mentioned in paragraph 3.23 (iii), organizations will have the obligation to ensure the accuracy of the data. It may therefore, require an organization to inquire if an individual is living or deceased.

Another situation mentioned in paragraph 3.23 (iv), the organizations are required to allow the consumers to have access to their data and for the data to be corrected if the data is incorrect or inaccurate. If there is a request to access the personal data of deceased individual by a third party, the organization is required to confirm whether an individual is living or deceased. The third party may be required to provide some evidence that the individual is deceased before organization releases the data.

Furthermore, based on paragraph 3.23 (i), the organizations are required to notify and inform the consumers whether the organization is processing his data and the purpose of the processing. Thus, this 'notification' requirement would have no application to deceased individuals.

If the proposed DP law is to cover personal data of deceased individuals, it is not workable to do it by simply defining personal data to include of deceased person. Specific provisions are required to be incorporated into the DP Act to provide certain rules pertaining to the use and disclosure, access, accuracy and security of the data.

C. Question 5: Do you have any views/comments on the proposed organizations covered by the DP law?

As mentioned in paragraphs 3.1 (a), 3.18, and 3.19, the proposed DP law will govern only private sector organizations. The reason for excluding the public sector, as mentioned in paragraph 3.18, is that the public sector is already governed by the internal rules and regulations regarding DP.

Thus, there will be two different DP regimes in Singapore. There is a need to make an assessment on these internal rules and regulations governing the public sector. Do they provide adequate protection as the proposed DP law? Are they compatible with the proposed DP law? Paragraph 3.18 states that "the public sector rules accord similar levels of protection for personal data as the proposed DP law". A thorough evaluation will have to be undertaken.

The questions mentioned above are very crucial in relation to a situation where a private company needs to share personal data with a government entity. So, in

this scenario, the private company will be subjected to this proposed DP law and the government agency will be governed by its internal rules and regulations.

This issue is also important in relation to the issue of transfer of data into Singapore by organizations located outside the country. Article 25 of the European Data Protection Directive, for example, states that the transfer of data to outside Europe can only take place if that country provides adequate protection. If it involves a transfer from the European entity to public agency in Singapore, the internal rules and regulations concerned must provide “adequate” protection before the transfer can take place. And if it involves transfer between companies, the DP law will be evaluated.

The analysis of “adequate” protection under the European Directive will be based on both the content of the rules contains in the DP law and the means of ensuring their effective application. Simply put, adequacy appraisal will be based on the ‘content’ principle and ‘procedural/enforcement’ requirement.

The “content” principle outlines the basic data protection principles that any data protection law must have. They are: (1) the purpose limitation principle, (2) the data quality and proportionality principle, (3) the transparency principle, (4) the security principle, (5) the right of access, rectification and opposition, and (6) the restriction on onward transfer. Apart from these six principles, the additional principles to be applied to specific types of processing are: special handling of sensitive data, possibility to opt-out from direct marketing, and special rules for automated decision-making.

Paragraph 3.23 of the Consultation paper clearly states the data protection principles that the proposed Singapore DP law would have. All the six principles will be covered. However, in relation to (6) on restriction on onward transfer, paragraph 3.61 states that Singapore will adopt a “principle based” approach, leaving it to the data exporter to take appropriate measures to protect the data when transfer it to outside Singapore. Perhaps, a similar approach will be adopted with regard to transfer of data into Singapore.

A better approach is for the proposed DP law to have some rules and regulation on data transfer either outbound or inbound. The enactment of the DP law provides the opportunity to address this issue and other issues at the national level. By doing so, there is no need for each company in Singapore to deal with it individually. This opportunity should not be missed.

Two matters are unclear from the Consultation paper. Firstly, whether the rule on automated decision-making will be incorporated into the proposed law, and secondly, whether there will be specific rules on the processing of sensitive data. This matter and other matters briefly discussed above may lead to the decision that the DP law might not be adequate from the EU perspective.

D. Question 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 organizations 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 organizations?

It is suggested that the DP law should be applicable not only to organizations located in Singapore but also to organizations located outside the country if they process data in Singapore. For a company located in Singapore, the organization must be established in Singapore. This should be clearly stated in the proposed DP law. The word to be used is “established” rather than “located” in Singapore. The collection or processing is taking place “in the context” of the Singapore establishment. This is to make clear that the processing is taking place under the control of the Singapore establishment or for the purpose of further processing by the Singapore establishment.

For the organizations located outside Singapore or not establish in Singapore, the DP law should be applicable to them if they have equipments in Singapore, and they process and carry out processing within Singapore. This would mean that foreign organizations or companies that operate servers in Singapore would be bound to comply with the proposed DP law.

This would build consumers’ (Singaporean and/or foreigners) confidence that their personal data in Singapore is protected, which is very fundamental in achieving the second objective of the DP law - to strengthen Singapore’s overall economic competitiveness and enhance Singapore’s status as a trusted hub and choice location for global data management and processing services (as mentioned in paragraph 3.1 (b)). Specifically, this could make Singapore more attractive to companies to establish data centers in the country. More

importantly, this would encourage the outsourcing activities as well as cloud computing in Singapore.

E. Question 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 for artistic and literary purposes should be provided for?

The basis and rationale for the exemption or exclusion is to strike the right balance between the public interest in freedom of expression and the public interest to adequately protect personal data.

International instrument such as EU Data Protection Directive contains express exemption for artistic and literary purposes. The Directive provides that Member States shall provide for exemptions or derogation from certain provisions of the Directive for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

The OECD Guidelines do not provide specifically for an exemption or exception relating to literary or artistic purposes. However, the Guidelines recognize that there may be exceptions to the privacy principles, which should be “limited to those which are necessary in a democratic society”. Arguably, exemption for journalistic, literary and artistic purposes may fall under this as freedom of expression is a fundamental element of a democratic society.

The APEC Privacy Framework does not contain exceptions for journalistic, literary or artistic expression. However, it allows exceptions to privacy principles, provided they are to be: ‘limited and proportional to meeting the objectives to which the exceptions relate’; made known to the public; or in accordance with law.

At the national level, the Privacy Act of Australia exempts ‘media organization’ from the operation of the Act. In Canada, the personal information protection principles do not apply to personal information collected, use or disclosed by a private sector organization for journalistic, artistic and literary purposes. In the United Kingdom and Malaysia, only the security principle applies to data processed for the purpose of journalistic, artistic and literary purposes. The rest of

the data protection principles are not applicable to the processing of personal data for those purposes. In simple words, it is a partial exemption. The conditions are:

(a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,

(b) the data controller/data user reasonably believes that, having regard to the special importance of the public interest in freedom of expression, publication would be in the public interest, and

(c) the data controller/data user reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

It is suggested that flexibility is to be given to the processing of personal data for the purposes of journalistic, artistic and literary purposes. Apart from encouraging freedom of speech, this will promote organizations and individuals in Singapore to be more creative and innovative. However, a total exemption (none of the principle apply) or exempting the organizations involve in the activities of journalistic, artistic and literary purposes from the operation of the DP Act are not the best approach to be adopted. It is suggested that the position taken by the U.K and Malaysia is to be considered. Firstly, the security principle is still applicable, which means that organizations that process data for the purposes of journalistic, artistic and literary purposes are required to take measures to ensure the security of the personal data. Secondly, to strike the right balance, certain conditions need to be attached to the exemption.

F. Other Matters

Complaint-based approach

Paragraph 3.5 indicates that the approach to be adopted is “complaint based”, which means that the DPC will investigate cases of non-compliance based on complaint. The justifications given for this are: to keep compliance costs manageable, to reduce the resources needed to administer the regime and to allow efforts to be focused on more significant data breaches. It is acceptable, as mentioned in paragraph 3.5, that the DPC will not regularly audit the organizations. The organizations themselves will have to do it in combination with

the other audit exercises obligated upon them. However, confining the investigation solely base on complaint by the consumers may not be good enough.

A complaint-driven enforcement may not be an effective way to enforce the DP law. The inability of potential complainants to recognize breaches and their unwillingness to complaint can be the obstacles to enforce the DP law effectively. It is suggested that the DPC be allowed to investigate breaches or potential breaches on his own initiative.

Only consumers' data

As mentioned in paragraphs 1.3, 2.6, 2.7, 3.1 and throughout the Consultation Paper, the proposed DP law is to cover only consumers' data. One of the key objectives and principles of the DP law, as clearly stated in paragraph 3.1, is to "ensure adequate safeguards to protect consumers' personal data and promote greater consumer trust in the private sector." Data protection law, however, is about privacy which has been regarded as human right under Article 12 of the United Nations Declaration of Human Rights 1948. Data protection is an informational privacy, which gives right to an individual to have control over his or her information or personal data. It is about "individual" and not "consumer". An individual may or may not be a consumer.

Restricting the DP law to consumers only may cause difficulty in certain circumstances to determine if someone is a consumer. For an example, is an employee a consumer? How about users of free services? In India, in the context of Consumer Protection Act, the Supreme Court has held that doctors and hospitals rendering service on payment basis to all persons, as well as those providing free medical service to some poor patients but rendering bulk of medical service to patients on payment basis would fall within the purview of the Act. However doctors and hospitals rendering service without any charge except nominal registration charges would fall outside the purview of the said Act, and consequently, users of such free service would not fall within the definition of consumer.

The uncertainty may also arise in relation essential commodities users, legal representative of deceased consumer, individuals with CPF savings, owners of

HDB flats, students (school, college and university) , a partner of a registered partnership firm, potential user, shares and debentures holders in a company, etc. Are they “consumers” for the purpose of the DP law? Uncertainty can make the DP law weak and insubstantial.

Restricting the scope of the DP law only to consumers’ data may not be the best approach to adopt. It is suggested that the DP law should cover individuals’ data rather than just consumers’ data.