EuroCham
Singapore
European Chamber of Commerce

MEMORANDUM

Public Consultation by MICA on Proposed Consumer Data Protection Framework for Singapore –

Response by EuroCham Singapore dated 25 October 2011

EuroCham Singapore is grateful of the opportunity to provide a response to the consultation paper dated 13 September 2011 on a data protection law proposed for Singapore.

EuroCham Singapore is the voice of European business in Singapore. EuroCham Singapore's ICT Committee takes a keen interest in the ICT sectors. It aims to help strengthen the economies in which our members have invested by supporting pro-competition, free trade and investment policies which attract capital and skills. In doing so, we recognise the important hub status of Singapore. Further details on the aims and role of our ICT Committee can be found at:

http://www.eurocham.org.sg/index.php?option=com_committee&task=view&id=5&Itemid=54

Our response is ***structured*** as follows:

A. – Covering letter with contact details – in a separate PDF file

B. – Summary of major points, and general comments

C. – Specific comments and responses to specific questions

D. – Conclusion

B. Summary of major points, and general comments

1. We support business-friendly policies; and these can and should sit well with the protection of personal data. Confidence in the jurisdiction is important for Singapore as a business hub. Other elements such as a reputation for accurate data should further enhance Singapore's standing.

2. We agree with the principle of balance described in para 1.2 of the Consultation Paper: legitimate and reasonable purposes for use of data is to be balanced with an individual's valid expectation that his/her personal data will only be used for known and reasonable purposes.

3.The consultation paper notes a number of proposed exemptions and scope boundaries which recognise the existence of other similar laws applicable to the public sector or specific industries. It will be impossible to achieve perfect 'dovetailing', thus we assume that the rule would be that in the case of inconsistency (ultimately), the higher obligation will prevail.

Prior to the stage of drafting a proposed law, we recommend review with other agencies, regulators and licensees so as to minimise duplication and conflict. Thus a second round of consultation will be useful, given the large impact that a DP law would have.

Where in certain cases a law seems premature or the outcome is too uncertain, consideration could be given to the use of a Code of Conduct, with voluntary adherence using a ‘comply or explain’ method (an example being the process used for the Corporate Governance Code applicable to SGX listed entities). We draw no distinction in our comments between primary legislation (Act of Parliament) and secondary (regulation) – see para 4.10, but note that a Code or Guidelines may be more appropriate in some cases following our suggested review.

4. We would suggest that further clarity of thought is needed around the regulation of Collection; Use/Process; Disclose, which are different acts. Consent should be considered in a structured way, as is often the case in practice today (eg consent to create and use the data internally, but not to disclose it, or only to disclose it for defined purposes). Paras 3.39 to 3.61 are relevant.

5. Further consideration is needed about the use of data in an aggregate or anonymised way. Thus while a DP law may apply to collection of data about an individual, including transaction data (eg mobile phone calls, credit card purchases, other transactions which may not currently be separately regulated), obtaining consent to subsequent use of anonymised data may not be required, depending on whether it identifies the individual.

6. Further clarity is needed as to when consent is deemed or implied, vs when an exemption to obtaining consent applies. Thus for employee data – what is appropriate? – consent to collect and retain may be more appropriate than exemption.

7. Singapore aims to be well positioned as a consumer insights and analytics hub. In addition to Singapore’s data hosting attractiveness, programmes such as MDA’s Interactive Digital Media and SMU’s LARC (coupled with EDB promotion of such activity) mean that analytics and related fields should grow. The data may or may not include data about Singapore citizens or residents and the base data may not have been collected in Singapore. We consider it important that the DP law adds value to this industry. An exemption for research and business analytics (para 3.56) may not thus provide the reputational quality assurance which would best support these aspirations, nor may a simple jurisdictional definition which excludes data created outside Singapore. Rather, consideration should be given to security requirements applicable to custodians and processors of such data, on a ‘best standards’ or ‘best practices’ basis rather than strict liability basis. The value of the OECD Model Data Protection Code to the TrustSg initiative (see para 2.4 and n.6) is a useful analogy. Singapore should not become a port of convenience for lax standards in data security, nor a place where known loopholes in the DP law can otherwise easily be circumvented.

Most importantly, the discloser (which is within the scope of the DP law) should not be exempt or exonerated just because the data is outsourced by disclosure to a third party. If the processor (disclosee) is under a data security obligation, but the discloser is under the main obligations in the DP law, the two parties can work out their own business arrangement. Para 3.61 covers this where the data is transmitted outside Singapore.

8. As to extra-territorial and transborder issues, further clarity is needed as to the basis of scope of the DP law. Is it to be based on where the data is collected, where it is processed, whether it includes data about Singapore citizens and residents or some other basis?. The consultation paper goes some way towards clarity. Please also see our general comment 7 in this regard.

9. We would encourage the view that a sound data protection, data security and data accuracy regime will contribute positively to Singapore's business standing and done in a way which is not administratively burdensome or costly, will assist businesses in the data management ecosystem.

C. – Specific comments and responses to specific questions

Questions 1 and 2:

We agree that a standard should apply across all sectors (para 3.8) but please see our general point 3.

Organisations in the public sector should not be exempt, where they are carrying out operational activities. Please see our general point 3 – rather than exempt on the basis that existing legislation is already expected to cover the point, non exemption but a rule where the higher standard prevails in the case of conflict, will avoid ('lacunae') and loopholes.

Questions 3 and 4:

Data should include transaction data. Para 3.11 should exclude anonymised data (see our general point 5), provided it does not identify individuals – eg very small groups may only become apparent after processing. We have nothing to add at this point on data of the deceased other than to agree that its disclosure, retention or non-retention can affect living relatives. There are legal rules in place already for the legal representative of a deceased's estate to have access. Perhaps finding a mechanism to release it such representatives would be the answer.

Questions 5 and 6:

Please see our general points 7 and 8 and our response to questions 1 and 2. For data hosts, data security obligations at a minimum should apply.

Questions 7,8,9:

Exclusions: Some consideration is needed where a news organisation wrongly discloses, does that render subsequent disclosure by others permissible or exempt from coverage? If the definition of news organisation is broad, can wrong disclosure through an on-line blog be allowed?

Questions 10,11:

We are not sure that the proposed DP law does not draw a distinction between data controllers and data processors (para 3.28). It appears that data collected outside Singapore (which may include personal data about Singapore citizens and residents) is not to be covered by the DP law, even where that data is sent to Singapore for processing. Please see our general comments 3, 7 and 8. Again we note that some data security obligation on data processor (para 3.29) would positively contribute standing and would maintain quality in the industry.

As to consent, we would suggest generally that an ‘opt out’ approach is easier to administer (para 3.35), but it may need to be structured, as it often is in practice now. Para 3.31 is an example where collection, use and disclosure are bundled together. Please see our general point 4. This should not be an undue administrative burden on individuals provided the opt out option is clearly displayed – there could be a specific requirement for such clarity, with the kind of structured approach we have described earlier.

The test of ‘necessary to provide the product or service’ also needs further consideration. To be competitive, many organisations need to carry out analytics on their customer data. They may do so in an anonymised way (thus possibly changing the character of the data to be non personal, according to the proposed definition) or they may not but such activity is a necessary part of providing a good service and is thus ‘necessary’, or there is an allowance for reasonable extended use of data. Without clarity on this point, a business may claim a right to refuse to provide a service if the individual does not consent to the data being processed.

Para 3.38 – the designation could be of individuals or a section or division or section of the firm.

Questions 12,13,14:

We agree with the general approach in paras 3.40 and 3.41. However, please see our general point 4. There needs to be a requirement to allow opt out under contracts of adhesion, particularly about disclosure to third parties with the purpose stated,

- Eg ‘data will be used for marketing purposes’ would need more detail – to allow for opting out where it may identify the person even if only as part of a group, and be used for targeted campaigns; but where aggregated and no personal details are used – a firm need not be required to offer the customer opt out in such cases. See our earlier comments on the scope of ‘personal data’

- Can a customer change his mind – and again? – then what periods does the consent apply to?

- Consent to provide to third parties – this could also be opt out but is needed.

Para 3.45, 3.46 are examples where we consider it would be more useful to de-bundle collection, use and disclosure. In the instance of group data, it depends on intended use and disclosure. A general exclusion for credit bureau reporting may not be most helpful from an overall reputational point.

Para 3.49 – please see our earlier comments on data processing.

Para 3.56 – please see our earlier comments on this point.

Questions 14,15:

Para 3.64 refers to security obligations, with which we agree. We have earlier recommended that data processors which may not otherwise be covered as proposed in this consultation paper by the DP law, be under a data security obligation (see our general point 7).

Question 16

We agree with the overall need to maintain accuracy and would suggest that this will further enhance the business reputation of Singapore. Please see our general point 9.

One element of this is allowing individuals a right of access. We agree with the concept of cost recovery. The fee proposed in para 3.70 could be nominal for the first check of accuracy.

Whether the individual should have access to derived or analysed information is more complex. There may need to be a definition of what is accessible, or alternatively nothing which is maintained about the individual (eg internal reports) is excluded, but the list of possibilities in para 3.73 would seem to suggest that loopholes could be exploited.

There are reports in the local media about a credit bureau maintaining two files. There would need to be a means of avoiding this kind of loophole.

Questions 17, 18

We agree that the Data Protection Commission should be complaints-based (rather that using an audit regime) but the DPC could also take a pro-active approach in research and understanding of how the law and policy are operating.

Question 19:

Help, education and support would be our suggestion. DPC should have an education budget as should public sector to contribute to knowledge and compliance. DPC talks should be available at no cost to private sector.

Questions 20, 21,22:

We have no comments on the proposed transitional provisions at this stage.

Question 23 :

National Do Not Call registry. We consider that the obligation not to contact would be better done at an operator level at this stage, or through voluntary industry associations. We note the Contact Centre Association's Code of Ethics as an example of the latter.

D. – Conclusion

A sound data protection, data security and data accuracy regime will contribute positively to Singapore's business standing and done in a way which is not administratively burdensome or costly, will assist businesses operating in the data management ecosystem.

EuroCham Singapore is generally supportive of a base DP law. We have made recommendations about a more thorough review and some suggestions on a number of specific aspects.