Your Ref:
Our Ref:
Email: tim.pullan@taylorvinters.com

TAYLOR VINTERS
SOLICITORS
www.taylorvinters.com

Date: 25 October 2011
Tel:
Fax:

Ministry of Information, Communications and the Arts
140 Hill Street
#02-02
MICA Building
179369

Singapore
**By Email**

Dear Sirs

**Public Consultation of the Proposed Consumer Data Protection Regime for Singapore**

We refer to your request for feedback to the consultation paper dated 13 September 2011.

Our comments on the proposals are set out in the appendix to this letter. We have not attempted to pick up every potential issue, but focussed on the key points from our perspective and experience, and that of our clients.

Taylor Vinters are a law firm specialising in international technology and outsourcing transactions. This includes expertise in cloud infrastructure projects, traditional IT & telecoms infrastructure, cross-border data flows and marketing/BI data analysis and usage.

We believe that the position adopted by MICA in its proposals is appropriate, finding a delicate balance between the local needs of business and citizens and the requirements of Singapore's international trading partners and business interests. Inevitably there remain some important decisions, with a high priority on ensuring that the new law attracts business to the country.

We look forward to continuing our engagement with the Ministry on this initiative.

Kind regards

Tim Pullan
Consultant
**TAYLOR VINTERS**





SINGAPORE OFFICE
Level 40, Ocean Financial Centre
10 Collyer Quay
Singapore 049315

## APPENDIX

## Comments on Proposed Consumer Data Protection Regime

### General

*European adequacy finding*

One of the benefits of the new regime should be automatic recognition by key trading partners as a safe destination for personal data.

Europe has a mechanism for recognising jurisdictions with adequate regimes and maintains a "white list" (http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm).

As a key trading partner it will be useful if Singapore's new law and enforcement regime qualifies it for inclusion on this list. This is particularly the case for data processing and hosting businesses that locate themselves in Singapore, and also generally to support the perception that Singapore is a safe harbour for personal data.

To this end, we believe dialogue with relevant European Commission officials through this process would be helpful.

### 3.5/Question 1

We support the proposed complaints-based approach.

However, in some industries involving the storage and protection of personal data, compliance certification can help provide the necessary confidence to customers, here and abroad.

We suggest that the new DPC be given the powers to recognise and officially sanction audit/certification services provided by the private sector. The same comment applies to security measures (A3.64).

### 3.11/Question 3

One of the issues commonly experienced by business intelligence providers and their clients under European data protection law is that data files which contain no personally identifiable information are still considered personal data if the company holds separate information which taken together with the data file would enable people to be identified.

This is the case even where the company has established firewalls between both sets of data to prevent identification.

The ability to be able to perform analysis on anonymous data sets often with multiple third parties to generate behavioural and other type of intelligence is key to the data industry.

We recommend that the definition of personal data specifically permit companies to store anonymous data separately from personal identifiers and not have to consider that data as personal data provided appropriate security and process firewalls to keep the identifier data separate are in place.

**3.22/Question 6**

We believe that Singapore's data protection law should apply equally to foreign organisations to prevent potential discrimination against Singaporean companies competing for the same business.

Applying the law in such a way would also go some way to deterring businesses based outside Singapore from being able to pursue "cowboy" marketing tactics in their pursuit of Singaporean custom. Otherwise, the benefits to the typical Singaporean consumer of the new regime may be reduced.

Enforcement action relating to privacy breaches by a foreign company affecting foreign individuals is likely to be uneconomic in most cases. We assume the DPC can be provided with the discretion to decide not to act in such cases.

However, enforcement action relating to breaches by foreign companies targeting Singaporean consumers may be more realistic.

**3.28/Question 10**

It is important that pure data processors are not themselves subject to the new law in relation to client data that they process.

The reason for this is that providers such as hosting and cloud providers often rightly have no knowledge or understanding of the personal data that passes through their systems. To impose such an obligation would place such companies at a competitive disadvantage against competitors in other countries, including Europe and the US.

The mechanism under European law – where data processors are not directly subject to the data protection regime, but companies that use their services are legally obliged to impose specific contractual obligations on them with regard to security and other matters – has proven to work well in practice over many years. We recommend that consideration be given to adopting a similar regime in Singapore.

These comments apply having also considered the proposed exclusion of consent requirements in outsourcing situations (paragraph 3.48).

**3.31/Question 10**

Personal data has an economic value for marketers. Should companies be prevented from selling consumers valuable products and services, in exchange for the right to use their personal data?

**3.42/Question 12**

We believe that organisations should be able to obtain consent as soon as practicable after first use or collection, including where the data is being used for marketing, and provided that it has not been obtained in breach of the Act.

An example is where a company has consent from its customers to disclose their data to a third party company for marketing purposes. To comply with the new law, the third party may need to obtain additional consent to commence marketing, but cannot do so without first contacting the individuals concerned.

**3.67/Question 15**

Our view is that the task of specifying retention periods upfront and then managing storage and deletion processes in line with those retention periods will be too difficult and complex for most companies to comply with. As a result, we believe that there would be widespread delinquency against this obligation that would make enforcement impractical.

Companies should have the general obligation to review data retention and regular intervals and delete data that is no longer required.

**4.1/Question 17**

It would assist effective enforcement if the DPC is given the power to take action in confidence, without the need to publicise all such steps. This may already be an implied area of discretion.

**Conclusion**

We believe that the current position adopted by MICA in its proposals is appropriate, finding a delicate balance between the local needs of business and citizens and the requirements of Singapore's international trading partners and business interests. Inevitably there remain some important decisions, with a high priority on ensuring that the new law attracts business to the country.