Allen & Overy LLP

**MEMORANDUM**

To MICA_DP_Public_Consultation@mica.gov.sg

From Allen & Overy LLP Singapore

Our ref PERSONAL-# SN:4482376.1

Date 25 October 2011

Subject **Public Consultation issued by the Ministry of Information, Communication and the Arts – Proposed Consumer Data Protection Regime for Singapore**

## We support the introduction of a general DP regime and general comments

1. We welcome and support the Government's proposal to introduce a general DP regime for Singapore, and appreciate the opportunity to comments on the Consultation Paper dated 13 September 2011 (**CP**).

2. We agree with the need for the new DP regime to target consistency with international standards.

3. However, we would suggest respectfully that it may be better for the proposed new DP regime not to define itself as being (to use expressions of the Consultation Paper) primarily a "light touch", "baseline law" aimed just at setting "minimum standards of DP across the private sector". This would lead to an incongruity in terminology which may lead observers to wonder if the new DP law would in fact enable Singapore to claim that our new regime "... will put Singapore *on par* with other advanced economies that have introduced DP laws."?

4. Therefore, we would respectfully suggest that the DP regime seek to orient itself as seeking to attain *best practice*, while at the same time being give due respect to the need to balance potentially conflicting objectives, including on the one hand various needs of individuals

served by data protection laws (such as harm prevention and privacy) and on the other countervailing societal benefits that may arise from information sharing and the avoiding of un-necessary compliance costs for businesses.

5. We do not believe that the differences between the stances in paragraph 3 and 4 are merely about semantics. The underlying philosophical stances of the new DP regime matter and it is important to express it clearly.

6. Specifically with regards to the goal of minimizing compliance costs, we agree with the approach whereby the Data Protection Commission (**DPC**) would focus on educating businesses and the public and on investigating complaints and more significant data breaches instead of programme of "regular" audits. We would presume, however, the DPC would retain some powers to conduct audits of specific organizations where deemed appropriate. Is this correct?

**Relationship with sectoral regulation**

7. The above suggestion is also not meant to imply that we favour the view that the general DP regime should wholly supersede specific sectoral regulation. In regard to the relationship between the general DP regime and sectoral regulation:

   (a) we agree that **higher standard sectoral regulations should remain** – For instance, the Banking Act (Cap. 19) currently imposes a *blanket* prohibition on disclosure of any "customer information" and this kind of enhanced sectoral regulation serves a useful function and should continue to co-exist with the new general DP regime.

   (b) we note that the existence of a specific sectoral regulation **does not pre-empt the general DP regime, unless the sector regulator requests an exemption from the DPC** – for example under Part II Para 7 of the Third Schedule to the Banking Act, information obtained by a bank may be disclosed to a credit bureau *without customer consent*. However, it would seem that the obligations under the new DP regime would not be pre-empted by the exceptions to banking secrecy contained in the Third Schedule to the Banking Act, unless MAS as sector regulator applies to the DPC. If this is the case, it may be useful for the key sector regulators to give consideration to the kinds of exemptions which they may need to seek from the DPC at the time of commencement of the DP regime, and for the DPC to publicly disclose such anticipated applications for exemption in its response to the CP. Alternatively, specific exemptions may be granted under the DP legislation. For example, it may be provided that the no consent is required for disclosure of customer information permitted under the Third Schedule to the Banking Act.

   (c) **piecemeal nature of sectoral regulation emphasizes key role of general DP regime** – The fact remains that sectoral regulation is inherently piecemeal in coverage (i.e. the majority of sectors are *not* covered by specific sectoral regulation). Therefore, the importance of the general DP regime should not be under-estimated.

8. On the whole, it seems to us the proposed DP regime is broadly successful in striking a reasonable balance between the competing considerations. The new DP regime also appears to contain a *prima facie* effective penalty and enforcement regime, although how things will actually work in practice would naturally need to be seen.

**Providing for the flexibility not just to set reduced standards, but to impose enhanced ones**

9. Given that the DP regime is new in Singapore, we believe that the DP legislation should include general mechanisms whereby the Minister-in-charge should be empowered to grant new exemptions to loosen the baseline requirements where this is appropriate.

10. Conversely, in our view, it may also be worthwhile to build in some flexibility in the DP legislation allow the Minister-in-charge to prescribe by regulations *enhanced* standards to be applied to certain categories of data or to certain circumstances. Bearing in mind the concern noted in **CP Para 2.6** that:

> "... there is a growing concern that consumers' personal data is being sold or used without their consent [which] is exacerbated by new technologies that create potential for infringements of consumer privacy even as they develop new opportunities to improve everyday life",

giving the DP regime a degree of flexibility to introduce new or enhanced requirements *in future* may allow the DP regime to better cater to evolving needs and standards. The legislation should allow such higher standards for *opt-ins* but the possibility to impose mandatory standards (for example, requiring express consents for certain kinds of certain sensitive data or certain personal data collection processes) should perhaps not be excluded (if thought necessary, subject to appropriate safeguards)

11. We would also suggest that it would be better if the initial list of exemptions be set out in subsidiary legislation, instead of the primary statute, for ease of future refinement and amendment, to suit changing circumstances or as experience is gained with their operation.

**Types of data covered**

12. **CP Para 3.16** – We are in favour of the view that personal data of a deceased person should not be covered by the DP regime, for the reasons set out in **CP Para 3.15**. This is consistent with the position under the current Model Code.

**Types of organizations covered – Public sector and persons other than organisations in Singapore**

13. We agree that the needs and circumstances of the public sector and the private sector do differ considerably. However, while the CP Paper correctly states that it is common internationally for distinct legal regimes to govern the public and private sector, it is also true that the public sector is in many advanced economies subject to some general DP

discipline under the law[1]. It is true in the case cited of Malaysia, the Personal Data Protection Act (passed in 2010) is a DP regime which only applies to private sector organizations, but we would respectfully query if this approach can be said to fully reflect the prevailing international consensus. Canada was the other example which was cited, but in that case, the DP regime for the public sector ***is*** governed by statute, namely the Privacy Act, and, for example, one of the purposes of that laws to "... provide individuals with a right of access to [personal information held by government agencies].". Hence, even in Canada, statute does impose DP legal disciplines on the public sector. The overriding issue therefore with respect to what DP regime should apply for the public sector is not so much whether the same law applies to both, but rather the key question is the extent to which the public sector should be made subject to equivalent standards and disciplines that apply to DP in the private sector, including:

(a) the provision of access to individuals in respect of information held by government agencies about them;

(b) the principle of limiting collection;

(c) the principle of reasonableness;

(d) the provisions on accountability;

(e) the duty to ensure accuracy,

etc.

while taking into account real differences between the legitimate requirements of the public and private sectors (for example, the special needs of investigative and security agencies). Clearly, by virtue of the Official Secrets Act (Cap. 213) and the Statutory Boards and Government Companies (Protection of Secrecy) Act (Cap. 319), the aspect of DP relating to confidentiality of officially held personal data is currently well-protected. It may be asserted that public sector agencies are subject to internal rules that are analogous in some respects to those that apply to private sector organizations, but with due respect, it is far from clear that an adequate degree of equivalent protection would arise simply from reliance on internal rules of Government agencies. In principle, we believe that the Government ought to be willing, subject to different treatments necessitated by legitimate public requirements, to subject personal data held by its agencies to the *same standard* of discipline as private sector bodies are. This would be the true demonstration of "walking the talk".

14. As for whether the DP regime should apply to a person other than an organization operating in Singapore which processes data in Singapore (for example, by virtue of having a computer in Singapore), we note the CP referred to the debates within the EU on this issue. However, given the practical difficulties in implementing such a regime in Singapore, which

[1] See ***OECD Privacy Guidelines – Thirty Years in the Private Sector***

we believe are likely prove significant in practice, it would probably be more practical at the initial stage to apply the DP regime only to organizations in Singapore.

**General rules**

15. **CP Para 3.29** states that "an organization that outsources the collection and/or processing of personal data is still responsible for the management of such personal data". The extent of an organization's responsibility should be defined clearly. For example, is the outsourcing organization:

    (a) "vicariously" responsible for any data breaches by the data processor;

    (b) responsible for selecting with due care the data processor;

    (c) responsible for oversight of the activities of the data processor;

    (d) responsible for assessing the adequacy of the data protection regime in the jurisdiction of the data processor. etc. (note in this regard that we agree with the proposal in **CP Para 3.61** that adequacy rulings for cross-border personal data transfers should *not* be mandated)

    If the general intent is that where personal data processing is outsourced, the organisation outsourcing the processing of personal data is required to *take reasonable steps to ensure* that the personal data which is to be transferred will not be dealt with consistently with the DP regime (see the current Model Code), this should be made clear.

16. **CP Para 3.29** also suggests that an organization which processes personal data as an outsourced service provider may have "control" over the personal data. It would be useful to clarify the intended definition of "control" (and for that matter "custody") in this regard. In the Model Code, for example, "control" is defined as "power to determine the purposes for which data are processed and the manner in which they are processed." If this definition were to be adopted, it may not apply to an outsourced processor.

17. **CP Para 3.35** – In principle, we have no strong view on whether an "opt-out" facility should be permitted. However, it may be noted that since the CP currently does not propose any particular *mode* by which consent has to be given (and furthermore does not intend to provide that any particular information should be subject to enhanced safeguards, such as a requirement for express consent for sensitive data), the "opt-out" facility ultimately boils down to just another mode of consent. If this analysis is correct, then it should follow that "opt-out" facilities ought to be permitted as a consequence of the non-prescription of any particular mode of consent under the DP legislation. However, in the event that an "opt-out" approach is permitted, it would seem reasonable for the DP regime to require the organization to take reasonable steps to highlight to the individual the terms of consent deemed to be given if no "opt-out" is exercised, the existence of the "opt-out" provision, and to put in place a mechanism that is reasonably practicable and convenient for the individual to exercise such a right of opt-out.

18. **CP Para 3.36** provides that an individual may withdraw consent at any time, unless such withdrawal would "frustrate" the performance of a legal obligation. The term "frustrate" may impose too high a bar in this connection. It may be better to provide, for example, that the right to withdraw consent is not applicable if this would "have an adverse impact" on the performance of a legal obligation by the organization possessing the personal data, which the organization cannot reasonably avoid without incurring costs.

**Rules on the collection, use and disclosure of personal data**

19. **CP 3.42** provides that personal data may be collected where it is reasonable to expect that the collection with the consent of the individual would compromise the availability of the personal data and the collection is reasonable for an investigation or legal proceeding. It would be useful to clarify if the intention is to cover all forms of investigation and legal proceedings, whether involving public sector officials or only private persons and whether civil, criminal or administrative. This point also relates to the exemption for collection of data to provide legal services to a third party referred to in **CP 3.46**.

20. In **CP Para 3.53**, the exemption should provide for disclosures by an organization to any of its professional legal advisers (including in-house counsel employed by the organization or another member of its group) for the purposes of or in connection with obtaining of legal advice or for the purposes of legal proceedings. The exemption should not be limited to advocates & solicitors qualified to practice Singapore law.

21. In **CP Para 3.58**, the obligation on the disclosing organization should be to *take reasonable steps* to notify employees, customers, directors, officers and shareholders whose personal data is disclosed. This would help to cater to situations where, for example, customers whose personal information must be disclosed are uncontactable.

22. We note that the CP does not clearly endorse that the principle of "**Limiting Collection**" (in the sense used by the Model Code) will apply under the DP regime, although this seems to be *implied* by the provision in **CP Para 3.66** that personal data which is not necessary for the stated purpose should no longer be retained. It should be clarified that it is the intention of the DP regime that this principle should be applicable..

**Rules on accuracy, protection and retention of personal data**

23. The requirement in **CP Para 3.63** to ensure accuracy/updating of personal data which "... is likely to be disclosed to another organization" may create difficulties in practice. For example, if a business transaction is proposed to be entered into between two organizations, will the first organization become obliged to update its database of personal data?

**Rules on access to and correction of personal data**

24. **CP Para 3.71** - We would suggest a caveat to the exception that access may be refused on the grounds that disclosure could, in the opinion of a reasonable person, harm the competitive position of the organisation, namely that it may be helpful to clarify that this

exception does not prevent an individual from seeking to verify the accuracy of information held by the organization, which information the individual already has in his or her possession (this basically reflects the principle of "severage" in Principle 9 of the Model Code).

25. **CP Para 3.73** - We suggest that the drafting of right to deny access there could be fine-tuned. The ability to deny access on the ground that the information requested is "trivial or not readily retrievable" seems wide, bearing in mind that there is already an exception proposed for disclosure "... where the burden or expense of responding to the request would be unreasonable or disproportionate to the risks to the interests of the individual."

26. A question may be asked whether an individual and an organization may, by agreement, restrict the use or disclosure of personal data except with the consent of the individual. It is suggested that nothing in the DP regime should *prevent* this, although an agreement between two private parties should, of course, not limit the powers of a government agency or the rights of a Court.

**Existing personal data**

27. **CP Para 4.17** – We note the proposal that consent should be *deemed* to be given by the individual concerned for an organization to use and/or process all existing personal data. Clearly, deemed consent should not apply to any personal data which was unlawfully obtained the organization (for example, in breach of confidence). We recommend that this point should be clarified.

28. While we should not be taken to express any strong view, MICA may wish to give consideration to the possibility of imposing a longer transitional regime, say 5 years, for existing personal data to be brought under the DP regime. If the transitional period were indefinite in duration, there may be difficulties to establish for many years to come whether any personal data of individuals is within the new DP regime or is not, since that would depend on the date of original collection which may be difficult to prove. The extent of this uncertainty over the protection offered by the new DP regime created by an exclusion of existing personal data for an indefinite period would therefore have to be balanced against the costs to enterprises of ensuring all their personal data comes within the DP regime within a longer transitional period.

29. We would also seek clarification whether what was intended by **CP Para 4.18** is that an organization would need to obtain a new consent if they wish to *disclose* existing personal data to a third party (e.g. by selling contact-lists), even if such data was previously used by the organization for the purpose of "sale" to third parties.

**Further consultation on draft legislation**

30. We would **strongly encourage** IDA to release the draft legislation for further public consultation before the new DP regime is enacted.

**Contact**

31. For any questions regarding this submission, please contact our Mr Yeoh Lian Chuan at +65 6675 6071 (email : lianchuan.yeoh@allenovery.com)