PUBLIC CONSULTATION OF THE PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE

SUBMISSION OF COMMENTS BY MEDIACORP PTE. LTD.

DATE OF SUBMISSION: 25 OCTOBER 2011

A. SUMMARY OF MAJOR POINTS

A short summary of the major points of our submission are set out below (references in brackets are to the corresponding paragraphs in the Consultation Paper).

1. Personal data for deceased persons should not be covered, or alternatively it should only be protected for a limited period of not more than 10 years (*paragraph 3.16*).

2. Whether Singapore-based organisations carrying out data collection and processing activities outside Singapore is within the scope of Singapore data protection laws (*paragraphs 3.20 – 3.22*).

3. The rules on accuracy and completeness of data and retention periods require clarification (*paragraphs 3.62 – 3.67*).

4. The rules on individuals' access to their own personal data should be limited, and only a best practice which does not attract legal penalties (*paragraphs 3.68 – 3.73*).

5. The DPC should be empowered to answer queries and issue clarifications on provisions of the Data Protection Act (*paragraphs 4.1 – 4.9*).

6. The "sunrise period" should be for at least 2 years to give organisations more time for implementation issues to be surfaced and resolved as the new legislation has wide ranging implications for business operations (*paragraph 4.14*).

7. More details are required on what is expected of organisations with respect to the proposed National Do-Not-Call Registry (*paragraphs 5.1 – 5.7*).

B. OUR COMMENTS

1. Personal data for deceased persons (*paragraph 3.16*)

1.1 We note that MICA is considering giving protection to the personal data of deceased individuals where such individuals have been deceased for less than 20 years.

1.2 We would propose that the protection of personal data should be limited to living individuals only.

1.3 As highlighted in the Consultation Paper, it would be administratively complex and costly for organisations to identify and deal with the correct parties authorised to make decisions in relation to the personal data of a deceased individual. Since there is no international best practice on this issue, it would not be unreasonable for Singapore to follow an established jurisdiction like the UK where their Data Protection Act only protects personal data of living individuals.

1.4 Even if it should be decided that personal data of deceased individuals should be protected for public interest reasons, we would propose that the protection period be limited to not more than 10 years to reduce the compliance costs for organisations.

2. Data collection and processing activities outside Singapore (*paragraphs 3.20 – 3.22*)

2.1 We note that the DP legislation would cover *Singapore-based* organisations carrying out data collection and processing activities *in* Singapore.

2.2 In this regard, we hope the new legislation will make it clear that Singapore-based organisations carrying out similar activities *outside* Singapore will *not* fall within the scope of Singapore's DP laws. We believe that should be the case as Singapore's DP laws should not have extra-territorial effect where the laws of other jurisdictions would apply.

3. Rules on accuracy and retention of personal data (*paragraphs 3.62 – 3.67*)

3.1 While we agree that organisations should make a reasonable effort to maintain the security of personal data which it has collected, it is not clear to us why it is necessary to require an organisation to ensure the data collected is "*reasonably accurate and complete*" (*paragraph 3.63*).

3.2 Any data collected can only be as accurate as what is provided to the organisation by the individual. Furthermore, organisations will collect personal data based on their business needs. So the question of whether the data is sufficiently "complete" should be decided by the organisation based on its own requirements, so long as the organisation complies with the relevant regulations on how such personal data can be collected.

3.4 As such, we are not quite clear as to the intent behind such a requirement and specifically what is expected of an organisation in terms of ensuring that data collected is "*reasonably accurate and complete*".

3.5 We also note that under paragraph 3.66, it is proposed that "*if an organisation uses an individual's personal data to make a decision that directly affects the individual, the organisation shall retain that information for a sufficient period of time after using it so that the individual has a reasonable opportunity to obtain access to it. Following that, an organisation shall then destroy its documents containing personal data, or make such data anonymous, when retention is no longer necessary for legal or business purposes, and as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data.*"

3.6 We are not quite clear what the above proposal is intended to address. So long as organisations are collecting and using the data in accordance with the relevant regulations, then the question of how long that data should be retained should be up to the organisations to decide based on their operational needs. Furthermore, individuals can always contact the organisations to withdraw their consent if they do not want the company to continue using their data. As such, we do not think it is necessary to have a rule on how long organisations can or should continue to retain such data.

3.7 We hope MICA will be able to clarify its considerations and give more details on what is required specifically in the next round of consultation, given that the above requirements will impose very onerous duties on business organisations.

4. Rules on access to personal data (*paragraphs 3.68 – 3.73*)

4.1 While we agree that organisations should be required to correct any inaccurate data at the request of the individual, we are not clear as to why there should be a legal requirement for organisations to give individuals access to their own personal data.

Such a requirement will give rise to significant increased costs for organisations and should therefore only be imposed if there is a significant benefit to the public.

4.2 Although it is also proposed that a reasonable fee may be imposed to recover costs, this is still only on a cost-recovery basis. Imposing such a requirement will become a heavy burden on most organisations which are already operating under very difficult conditions.

4.3 Even if it is deemed that individuals should have the opportunity to access personal data collected by an organisation, we would propose that this be a best practice guideline and not a legal requirement which attracts legal penalties.

5. Powers of the Data Protection Commission (*paragraphs 4.1 – 4.9*)

As this area of law is still relatively new to many organisations, we anticipate that many issues will arise as organisations take steps to comply with the new legislation. As such, we propose that the DPC be specifically empowered to answer queries from the public and to issue clarifications on the provisions of the Data Protection Act and any supporting codes, guidelines and regulations which may be issued.

6. "Sunrise" period (*paragraph 4.14*)

We would propose that the sunrise period should be for at least 2 years as the new DP legislation will have wide ranging implications for business organisations. Very often more issues will arise during the actual implementation process than what could have been anticipated previously. As such, having a longer "settling in" period will allow organisations more time to consult with the DPC and seek clarifications on the operation of the DP Act and its supporting codes and regulations.

7. Proposed National Do-Not-Call Registry (*paragraphs 5.1 – 5.7*)

7.1 We note the proposal to create a national DNC registry but we are of the view that more details are required on what is expected of organisations if such a registry is to be set up.

7.2 For example, how often will an organisation be required to check the DNC registry and update its records? If we have already obtained consent from an individual previously to collect and use his data, does the DNC registry override such consent? How does an organisation get specific consent to call an individual who is on the DNC registry, can the consent be express or implied? How easy or difficult would it be for an organisation to check the registry and match the DNC records against its own records, especially if the individuals on the DNC list run into the tens or hundreds of thousands?

7.3 We will therefore need more details before we can comment on whether it is feasible to have such a registry and the implications for our organisation.

C. CONCLUSION

1. We hope MICA will take into consideration our various comments as set out above in preparing the Data Protection Bill. While we welcome the introduction of a formal data protection framework in Singapore which will bring us in line with international best practices, business organisations in Singapore today are operating in an extremely fast-paced and competitive business environment and we need to be able to have the flexibility to move quickly to engage our customers and users pro-actively.

2. We look forward to reviewing the Data Protection Bill when it is made available to the public for further consultation next year.

3. Should you have any queries on our above comments, please do not hesitate to contact:

Ms Chng Bee Peng
VP, Legal & Secretariat
MediaCorp Pte. Ltd.
DID: +65 6350 3390
Fax: +65 6256 5555

4. Thank you.