SINGAPORE PRESS HOLDINGS LTD

Submission to the Ministry of Information, Communications and the Arts
on the Public Consultation of the Proposed Consumer Data Protection Regime for Singapore

25 October 2011

Contact Person:

Ginney Lim
General Counsel,
Executive Vice President
& Group Company Secretary
limmlg@sph.com.sg

25 October 2011

Ministry of Information, Communications & the Arts
(via email MICA_DP_Public_Consultation@mica.gov.sg)

Dear Sirs

PUBLIC CONSULTATION ON THE PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE

1. Singapore Press Holdings Ltd ("SPH") welcomes the opportunity to submit its comments on the Proposed Consumer Data Protection ("the DP") Regime for Singapore.

2. The comments set out herein by SPH are in response to the public consultation of the DP issued by the Ministry of Information, Communications and the Arts ("MICA") on 13 September 2011.

3. As a general comment, SPH is of the view that there should be a balance struck between the need to protect consumers' personal data and the value derived by organisations in collecting and using this data for their legitimate business objectives and purposes. In this regard, SPH is pleased to see that MICA has acknowledged that this is one of the objectives of the proposed DP regime and hopes that this intent will form the backbone of the new DP law.

4. In addition, SPH feels that the issue of compliance cost by organisations should be a key factor to be considered by MICA when reviewing the DP law or rules to be introduced into Singapore. SPH's detailed comments on the consultation paper and questions raised therein are set out below.

Summary of major points

5. SPH strongly supports the principle that key considerations in developing the DP would be to keep compliance costs manageable for businesses as well as to facilitate data flow instead of impeding it. This will allow local organisations to compete effectively against their foreign counterparts and on a level playing field.

6. SPH advocates that clear definition of personal data and exclusions be given either in the form of guidelines or within the new DP Act. If guidelines are to be given, these should be done concurrently when the new DP Act is enacted to allow organisations affected to better understand what policy or procedures need to be put in place to comply.

7. SPH would like to point out that as a regulated person under the Code of Practice for Market Conduct in the Provision of Media Services ("the Code"), it is governed and regulated under the Code which contains provisions on the use and protection of subscriber information or data under certain circumstances. It is submitted that in relation to subscriber information, the Code should prevail over the new DP law, and this should be made clear so that SPH may be able to comply with the relevant law.

8. SPH believes that the definition of personal data should not be extended to personal information about deceased individuals as it will be administratively complex, difficult and costly for organisations to identify and verify the parties who are able to act on behalf of the deceased individual in relation to obtaining consent.

9. SPH would like to highlight that leveraging on the personal data collected during the course of its business is an essential aspect of common business practice and commerce. There is nothing intrinsically objectionable with the collection of personal data. It is a basic principle of business economics for organisations to be able to leverage and mine the personal data collected from its customers. Some of these data collected are used by organisations to better service their customers and to cater to their ever-increasing demands, likes and dislikes.

10. SPH is of the view that the DP provisions should apply equally to foreign entities which collect personal data in Singapore. This is to ensure a level playing field and that Singapore-based entities are not prejudiced and able to compete fairly with their foreign counterparts.

11. SPH strongly supports the proposal to extend the exclusion to cover the use, collection or disclosure of personal data carried out by a news organisation in the course of a news activity. In addition, SPH supports the proposal to exclude collection, use or disclosure of a) an individual's business contact information, b) personal data solely for artistic or literary purposes, c) personal data recorded in documents for court proceedings, d) personal data about an individual in a record that has been in existence for at least 100 years (in this regard, SPH would recommend that the period be shortened to 20 years for practical purposes), and e) personal data under the control of a public agency or its agent. Further, SPH would like to advocate excluding the collection, use or disclosure of personal data which can be obtained from publicly available sources and requests

that guidelines be issued by MICA on what would constitute information from public sources.

12. Whilst SPH recognises that obtaining consent from individuals is necessary before it can collect, use or disclose any personal data, there will be practical difficulties in implementation and potential disputes, if MICA does not prescribe in detail the manner in which consent may be given in the DP Act.

13. SPH strongly supports the opt-out approach over obtaining consent approach. The opt-out approach will eradicate the practical difficulties which will be faced by organisations to authenticate whether consent had been validly given in the first instance.

14. MICA should not be too prescriptive about how organisations should ensure that personal data collected or used is accurate or complete, but should leave it to the organisations concerned as the interests are aligned to ensure accuracy and completeness.

15. Similarly, MICA should also not be too prescriptive about how to protect and secure personal data, and should be cognisant of the fact that despite the greatest of effort and will, the most secure information technology system may be breached or "hacked" into. Hence, organisations should not be held culpable if such inadvertent breaches or disclosures of personal data were to occur.

16. MICA should leave it to organisations to decide when to destroy personal data collected, from a practical and cost-effective standpoint. This is premised on the basis that organisations would not want to retain any data or information which no longer serves its purpose or which has become "stale" or inaccurate. There is again no need to be prescriptive about the retention period applicable for personal data of each individual, as common sense and practicality would prevail.

17. It is important that any access or correction rights of an individual to his or her personal data, should not unduly burden the organisation, such as disrupting its business operations and causing administrative burden or additional costs. Authentication of ownership issues may also arise in giving access to individuals and allowing them to correct personal data.

18. SPH would like to propose an informal guidance regime to be introduced whereby organisations may seek clarification and guidance with the DPC on whether the manner in which personal data is or proposed to be collected, used or disclosed, will be in breach of the DP law.

19. SPH believes that any financial penalty imposed should be based on clear provisions in the DP law for specified and serious breaches. SPH recommends that any financial penalty should be imposed only for

repeated offences, when notice for compliance has been given and there was non-compliance or flagrant and deliberate breach of the DP law.

20. SPH supports the proposed single "sunrise" period for organisations to comply with all provisions of the new DP Act and would suggest a period of two years as an appropriate and reasonable timeframe. Further, the proposal to exempt all personal data collected by organisations prior to the effective date of the DP Act from its provisions, is strongly supported.

21. Finally, on the National Do-Not-Call Registry ("DNC"), SPH feels that the current voluntary Code of Ethics put out by the Contact Centre Association of Singapore, with its comprehensive list of guidelines and the establishment of DNC lists in organisations, is more than adequate to allow individuals who do not wish to have unsolicited telemarketing calls an avenue to object to it. There is therefore no need for a separate DNC as it will be confusing. Organisations will need clarity as to whether consent originally obtained from an individual for the use or disclosure of his or her personal data has been superseded by that individual who has registered his telephone number with the DNC.

A. Key Objectives and Principles – Questions 1 and 2

22. Paragraph 3.5 acknowledges that a key consideration in developing the DP would be to keep compliance costs manageable for businesses and with this in mind, the proposed DP will be a baseline law to ensure that basic DP requirements are put in place by all private sector organisations.

23. Paragraphs 3.6 and 3.7 go on to state that it is important that Singapore's DP regime is consistent with international standards and benchmarked against that in other key jurisdictions.

24. SPH believes that as the DP is in its infancy stage in Singapore, caution should be exercised before we leapfrog and become on par with international standards. The EU, Canada and the US are way ahead of Singapore in terms of their privacy laws and DP rules, and are introducing more stringent measures. It is important to allow the DP in Singapore to evolve and for organisations to understand the impact on their business activities before introducing higher and more stringent standards. As we compete with countries in the region, it is also important that we should not be disadvantaged by the stringent and overly-restrictive rules placed on us in collecting and using personal data for our legitimate business purposes, when similar rules may not apply in these other countries.

25. Moving forward, SPH believes that Singapore will see stiffer competition, particularly as new technologies emerge and the consumer market becomes borderless. There should be a level-playing field in relation to reaching out to this growing borderless consumer market, and stringent DP rules which put obstacles in the path of businesses doing so, will only adversely affect our competitive edge. SPH therefore recommends a light touch in introducing a new DP regime.

26. In this regard, SPH does not agree that the more stringent measures proposed to be adopted by the EU and the US against the use of "cookies" and the proposed "Do-Not-Track" legislation respectively, should be adopted in Singapore.

27. SPH welcomes the statement in paragraph 3.8 that the DP law should facilitate data flow rather than impede it. In the light of this assurance, SPH has no objections to the concurrent application of the DP law with existing sectoral regulations, provided there is clarity as to which law or regulation should prevail.

B. Definition of Personal Data – Questions 3 and 4

28. The proposed definitions set out in paragraphs 3.9 to 3.11 do not give any certainty to organisations which will have to comply with the new DP regime.

29. Paragraph 3.12 goes on to state that the DPC may publish guidelines giving examples of information that may constitute personal data following the enactment of the DP law.

30. SPH strongly advocates that either the DP law prescribes the list of personal data that should be protected, or a comprehensive list of guidelines on what constitutes personal data should be issued at the same time the DP law is enacted. This will eliminate any ambiguity and will allow organisations to correctly address their resources to comply with the DP law and rules, instead of second-guessing them. SPH will urge that this be done concurrently with the new DP law and not at a later stage, even if a "sunrise" period is given for organisations to comply, as all organisations affected, will have to put in place policies and procedures to ensure compliance.

31. SPH favours the approach where any exclusion to the scope of what is regarded as personal data is clearly set out in the DP, eg business contact information or publicly available information, particularly from government agencies. This will provide more certainty to organisations for compliance purposes.

32. SPH would also like to point out that as a regulated person under the Code of Practice for Market Conduct in the Provision of Media Services

("the Code"), it is governed and regulated under the Code which contains provisions on the use and protection of subscriber information or data under certain circumstances. SPH would therefore like to seek clarification from MICA as to which should prevail in relation to its activities with regard to its subscribers. It is submitted that in relation to subscriber information, the Code should prevail over the new DP Act. It is also highlighted that at the time the Code was put up for public consultation in 2007, SPH had raised the issue that this provision in the Code should not be included therein and ought to be dealt with by the general privacy and data protection laws and legislation in Singapore at that time, but this was rejected by MICA then.

33. On the issue of whether personal data should be extended to personal information about deceased individuals, SPH agrees with the view that it will be administratively complex, difficult and costly for organisations to identify and verify the parties who are able to act on behalf of the deceased individual in relation to obtaining consent, and in relation to access and correction of personal data. For these reasons, SPH is of the view that adopting the approach by countries like the UK, where personal data of deceased individuals is not included in the DP, is preferred. We do not support the half-way approach of jurisdictions like Canada, which safeguards personal data of individuals for a period of 20 years after death for the reasons set out above.

C. Organisations and activities covered – Questions 5 and 6

34. SPH would like to emphasise to MICA the need to exercise restraint in implementing and applying this new DP regime to organisations in Singapore. In all industries and businesses, leveraging on the personal data collected during the course of its business is an essential aspect of common business practice and commerce. There is nothing intrinsically objectionable with the collection of personal data. It is a basic principle of business economics for organisations to be able to leverage and mine the personal data collected from its customers. Some of these data collected are used by organisations to better service their customers and to cater to their ever-increasing demands, likes and dislikes. Accordingly, this translates into direct benefits for consumers as better and more proactive customer service. Therefore, it is important that MICA realises that not all collection of personal data ought to be prohibited, and that some forms of this may actually bring about benefits for the economy and for consumers.

35. MICA must also be mindful of the larger consequences as companies regionalise or globalise, and take into account global competitive forces,

when imposing restrictions locally. Over-regulation and excessive restrictions in a small market stunt the growth of the local organisations, and render them ineffective when competing globally where scale and size matter.

36. On the issue of whether organisations outside of Singapore that engage in data collection and processing activities in Singapore should also be covered under the new DP regime, SPH feels that they should be. This will ensure a level-playing field for Singapore organisations and allow them to compete effectively in an increasingly borderless consumer-business environment in the face of technological convergence.

37. If local organisations and companies are to successfully compete with global companies and conglomerates, it is vital that they are not constrained in their ability to legitimately leverage on the consumer data they collect, particularly behavioural habits and preferences, through means like "cookies". This ensures that they are able to compete globally on an equal footing.

38. SPH is of the view that the DP provisions should apply equally to foreign entities, particularly those which have substantial resources and expertise abroad. It is important that such provisions apply to all persons who collect personal data in Singapore, including those located outside Singapore. This is to ensure a level-playing field and that Singapore-based entities are not prejudiced and able to compete fairly with their foreign counterparts.

39. However, SPH recognises that there may be difficulty taking enforcement action against such foreign companies or persons as they may not have assets in Singapore. It would be unfair if local companies are subject to enforcement measures while foreign companies are able to avoid sanctions under the DP law. Perhaps MICA will review its enforcement measures to see if situations where MICA is unable to enforce its decisions against foreign entities can be minimised, perhaps through cooperation with other regulators or authorities overseas.

D. General Exclusions from the DP law – Questions 7, 8 and 9

40. As stated above, SPH feels that all exclusions should be clearly set out in the DP law so that there is no ambiguity for compliance. The exclusions can be contained in the new DP law or in the proposed guidelines to be introduced on the definition of personal data.

41. SPH strongly supports the proposal to extend the exclusion to cover the use, collection or disclosure of personal data carried out by a news organisation in the course of a news activity.

42. SPH also supports the proposal to exclude collection, use or disclosure of a) an individual's business contact information, b) personal data solely for artistic or literary purposes, c) personal data recorded in documents for court proceedings, d) personal data about an individual in a record that has been in existence for at least 100 years (in this regard, SPH would recommend that the period be shortened to 20 years for practical reasons), and e) personal data under the control of a public agency or its agent.

43. In addition, SPH would like to advocate excluding from the DP restrictions, the collection, use or disclosure of personal data which can be obtained from publicly available sources, eg online or print directories like the Yellow Pages; the Singapore Exchange website on listed companies' information via their corporate announcements, annual reports, etc. disclosed to the public as well as to the Stock Exchange of Singapore; and data extracted from ACRA's company information. Clear guidelines as to what would constitute public sources should be established.

E. General Rules and Consent – Questions 10 and 11

44. SPH recognises that obtaining consent from individuals is necessary before it can collect, use or disclose any personal data. However, there are concerns if MICA does not prescribe in detail in the DP Act, the manner in which consent may be given.

45. These concerns relate to the authentication of such consent should a dispute arise as to whether consent was actually obtained.

46. In practice, organisations obtain personal data and seek consent for its use or disclosure through many different ways – online, verbally via the telephone, via short message system or sms, lucky draw or contest forms, etc.

47. Issues about how long should such consent be retained will be dealt with below under Question 15 – but at this point, SPH likes to highlight that if no guidance or specific provisions are made in the new DP Act in relation to the manner in which consent may be given, or the retention period of such consent by organisations – it would pose practical difficulties for organisations which have to comply with the DP Act. It is also unfair that little clarity or certainty is given to organisations, particularly if an

infringement of the DP Act may carry with it, a financial penalty of up to $1 million, as currently proposed.

48. Disputes are likely to arise when consent is obtained verbally and organisations may be forced to retain audio recordings of such verbal consent. However, even these may be subject to dispute, particularly if an individual challenges that the consent was not actually given by him or her over the telephone but by someone else.

49. SPH agrees with the opt-out approach adopted by jurisdictions such as British Columbia. This approach will certainly eradicate the practical difficulties which will be faced by organisations to authenticate whether consent had been validly given in the first instance. With this approach, individuals who have been notified of an organisation's intent to collect, use or disclose their personal data, may register their objections within a reasonable timeframe, and cannot later turn around to accuse the organisation of not obtaining its consent. To be fair to the individual, the new DP Act may provide that if an individual subsequently wishes to opt out, he or she may do so at any time by notifying the organisation, which must remove his or her personal data within a reasonable time. The procedures for opt out or withdrawal may be left to organisations to establish and such procedures should be made public, for example, through the organisation's website.

F. Rules on the collection, use and disclosure of personal data – Questions 12, 13 and 14

50. SPH agrees that it is neither practical nor productive to prohibit sharing of data in the circumstances set out in paragraphs 3.42 and 3.43. SPH is glad that MICA recognises that there are a multitude of data sources that could be considered publicly available, eg newspapers and directories, and that the DPC will provide further guidance on the types of sources that would be considered public.

51. SPH supports the proposal that the DP Act allows collection of employee personal data without the need for consent for the purposes of the employment relationship between the organisation and the individual. SPH however does not think it is necessary to notify the individual the purpose of collecting the data, as SPH is of the view that this will be a situation where consent is deemed to be given. It will be obvious to the individual when filling out a form applying for a job position in an organisation that the personal data being collected is for the purpose of the potential employment relationship.

52. Similarly personal data collected by organisations from their members for internal use or circulation should not be subject to the requirement to obtain consent, as it would have been obvious to the member when giving his or her personal data in applying for membership status, the purpose for which the data will be used. It will also pose an unnecessary burden and high compliance costs to the organisation should such consent be required to be obtained.

53. SPH agrees that it is important to extend the exception to research activities, including business analytics as this will support the drive to make Singapore a regional hub for businesses and emerging industries.

54. SPH also agrees that sharing and transferring of personal data in a merger or an acquisition should be an exception, but does not think it is necessary to notify each individual concerned that the personal data collected about him or her, has been disclosed to the party involved in the merger or acquisition. It would suffice that a public announcement or general notice or announcement is made to the organisation's employees, customers, directors and shareholders, informing them that a merger or an acquisition had taken place and that certain confidential information had been disclosed or shared in the said transaction.

55. In summary, SPH supports MICA's suggestions in paragraphs 3.42 to 3.48 and paragraphs 3.52 to 3.58, that for the situations mentioned therein, there is no need to obtain consent.

56. SPH would like to seek clarity on what would constitute "transfer of personal data outside Singapore". As acknowledged by MICA, this will become more commonplace with developments like cloud-based computing. Sharing of personal data will be usual between organisations within the same group or amongst related corporations in a group where some of these companies or organisations are outside Singapore. Insofar as it is practically possible, organisations, which use cloud-computing or other systems, would try to ensure that such sharing of data is secure or adequately protected. There may not be a deliberate or intentional transfer of personal data, but in the process of sharing information within the group, such personal data may be deemed to be "transferred" outside Singapore. The systems or cloud-computing used by the organisation may be infected by viruses or "hacked" into. SPH proposes that sharing within the group of organisations where some of them are outside Singapore, will be regarded as an exception to the principle of holding organisations responsible for the protection of personal data when it is transferred outside Singapore. Instead this will be governed by other provisions relating to personal data within the control of the organisation, such as safeguarding and protecting the personal data.

G. Accuracy, protection and retention of personal data – Questions 14 and 15

57. Although SPH agrees that it is important for organisations to ensure that the personal data collected and used is as accurate as is practicable, it likes to point out that if the individual providing the data does not provide accurate or complete data in the first place, organisations cannot be held responsible. Insofar as it is practicable, organisations would also prefer to collect and use personal data which is complete and accurate. MICA should not be too prescriptive about how organisations should ensure that personal data collected or used is accurate or complete, but should leave it to the organisations concerned as the interests are aligned to ensure accuracy and completeness.

58. On ensuring the security of personal data to prevent breaches and inadvertent disclosure, SPH has a similar view as in the previous paragraph, ie, MICA should not be too prescriptive and should be cognisant of the fact that despite the greatest of effort and will, the most secure information technology system may be breached. High-profile examples of such breaches have found their way in the newspapers recently, notable amongst them being the Wikileaks. Hence, SPH would advocate that organisations should not be held culpable or punished if such inadvertent breaches or disclosures of personal data were to occur.

59. SPH is of the view that the retention periods for personal data should not be so specifically tailored to each type of personal data collected, otherwise it will be impractical and difficult for organisations to implement. Organisations would have general retention periods for information or personal data collected and would destroy them automatically when these dates occur. To have to tailor or customise the period of retention for each individual's personal data and to inform each of them upfront, or even subsequently, what that period is, would be administratively cumbersome, and would impose too high a cost of implementation.

60. SPH advocates that MICA leaves it to organisations to decide when to destroy personal data collected, from a practical and cost-effective standpoint. This is premised on the basis that organisations would not want to retain any data or information which no longer serves its purpose or which has become "stale" or inaccurate. Moreover, there will be cost and space constraints involved for retaining data or information for too long a period. Hence, there is no need to be prescriptive about this as common sense and practicality would prevail.

61. SPH feels that the retention period need not be revealed to the consumer at the point of collecting the personal data, as long as the consumer has the right to withdraw consent or is availed of an "opt-out". Otherwise,

organisations will have to channel resources just to answer queries from customers who might have forgotten the retention period.

H. Access to and correction of personal data – Question 16

62. SPH is of the view that paragraph 3.68 is too prescriptive and will be unnecessarily burdensome on organisations, particularly the need to provide an individual with information about the ways in which the personal data has been and is being used by the organisation and the need to provide the names of the individuals and organisations to whom the personal data has been disclosed. It will be impractical, if not impossible, for organisations to keep track and a record of the names of individuals to whom the personal data has been disclosed, particularly if this disclosure is done in the course of its business activities and shared with employees or persons within the group of related companies, or with their out-sourced organisations and employees or agents.

63. Whilst SPH acknowledges that it is important that any personal data collected should be accurate and when corrected by an individual should be updated as soon as practicable, it feels that paragraph 3.69 is too prescriptive. It should be left to organisations to implement their own system of correcting such personal data in the most efficient and practical way.

64. SPH notes that the OECD model code provides for exceptions in allowing individuals to access their personal data, other than those circumstances set out in paragraph 3.72, such as commercial proprietary and contractual reasons. SPH advocates that such exceptions also be included in the DP law.

65. Another concern is the issue of authentication of the ownership of personal data before access is given or correction is allowed to be done. SPH recommends that where authentication cannot reasonably be carried out, organisations should have the right to deny access or reject any request for correction by a consumer.

66. Finally, it is important that any access or correction rights of an individual to his or her personal data, should not unduly burden the organisation, such as disrupting its business operations and causing administrative burden or additional costs.

I. Proposed penalty and enforcement regime – Questions 17 and 18

67. For greater certainty, SPH would like to suggest that an informal guidance regime be introduced whereby organisations may seek clarification and guidance with the DPC on whether the manner in which personal data is or proposed to be, collected, used or disclosed, will be in breach of the DP law.

68. SPH feels that there should be a cheap and efficient way of dealing with the concerns of the organisation being investigated or being asked to take corrective measures to ensure compliance, without having to resort to the appeals process. SPH would like to suggest that the DPC be given the powers to review or reconsider the corrective measures that it imposes on an organisation for compliance, when the organisation submits a request for reconsideration or review ("Reconsideration Request"). Hence any organisation aggrieved by any act, direction or decision of the DPC may request that the DPC reconsiders its act, direction or decision. In this way, it ensures that the enforcement process is flexible and fluid, and that there is an avenue for MICA or the DPC to address concerns that the corrective measures are unnecessary, burdensome or unduly broad.

69. The right to submit a Reconsideration Request ought to be included in the DP Act because of the severe penal consequences (such as the financial penalty of up to $1 million or the compensation to affected consumers as well as potential criminal prosecution) which flow from the failure to comply with the corrective measures imposed by the DPC.

70. SPH is of the view that any financial penalty imposed should be based on clear provisions in the DP Act for specified and serious breaches. SPH advocates that any financial penalty should be imposed only for repeated offences, when notice for compliance has been given and there was non-compliance or flagrant and deliberate breach of the DP law. Otherwise, corrective action or measures as directed by the DPC should be sufficient.

71. SPH does not agree that the DP law should provide that individuals may separately seek redress via civil proceedings in court. Such a right already exists for individuals to take civil proceedings if they are able to prove an actionable cause, but to have a specific provision in the DP Act may open the floodgates for individuals to bring organisations to court for compensation on the grounds of collection, use or disclosure of personal data without their consent. To prevent unnecessary legal costs and time being incurred in defending such civil suits, organisations may end up settling even frivolous and vexatious claims before they go to court, and may be the victims of "extortion".

72. SPH feels that as a deterrent, there should be a corresponding provision in the DP law to punish individuals who make frivolous and vexatious complaints against organisations. Otherwise, organisations may end up having to defend its actions to the DPC very often, and incur unnecessary costs and time in doing so.

73. SPH suggests that an organisation which is subject to investigative or enforcement action by the DPC, but which is also regulated by another regulatory body, may request or submit to the DPC that its actions are to be more appropriately investigated by the regulatory body.

J. Transitional Arrangements – Questions 19, 20, 21 and 22

74. SPH supports the proposed single "sunrise" period for organisations to comply with all provisions of the new DP Act and would suggest a period of two years as an appropriate and reasonable timeframe.

75. A two-year "sunrise" period will allow the DPC to educate the public and organisations affected about the proposed DP law and any guidelines pertaining thereto. It will also allow organisations with complex operations to harmonise their systems with the new regime. Organisations that are technology dependent or intensive will have to undertake the mammoth task of revamping and upgrading their information technology systems as well as restructuring their internal operations and information flow. During the two-year sunrise period, organisations can also put in place the appropriate policy and procedures to comply with the new DP law and instil awareness amongst its employees and other stakeholders.

76. This period of two years is not too long, and will be sufficient time to allow organisations to comply with the DP law.

77. SPH agrees with MICA's proposal in paragraph 4.17 to deem that consent was already given by the individual concerned for the organisation to use and/or process existing personal data, as this would certainly lower the compliance costs of organisations. Hence SPH strongly supports the proposal to exempt all personal data collected by organisations prior to the effective date of the DP Act from the provisions of the new DP Act.

78. As previously suggested above, SPH would like specific guidelines on what would constitute personal data and exceptions relating to its use, collection or disclosure for specified activities or circumstances, without the need to obtain consent from the individual affected.

K. Proposed National Do-Not-Call Registry ("DNC") – Question 23

79. SPH is of the view that the current voluntary Code of Ethics put out by the Contact Centre Association of Singapore, with its comprehensive list of guidelines and the establishment of DNC lists in organisations, is more than adequate to allow individuals who do not wish to have unsolicited telemarketing calls, an avenue to object to it.

80. To introduce another DNC within the DP Act will be confusing. Organisations will need clarity as to whether consent originally obtained from an individual for the use or disclosure of his or her personal data has been superseded by that individual who has registered his or her telephone number with the DNC.

81. If MICA is of the view that a DNC should be introduced, despite SPH's views above, then a separate consultation paper setting out the proposed detailed rules of the DNC is welcome. SPH reiterates that comprehensive guidelines are preferred to rules or laws with regard to the DNC regime.

Conclusion

82. SPH welcomes the opportunity to participate in the public consultation exercise for the proposed new DP regime. We hope that our views and the issues raised will be carefully considered and addressed by MICA.

83. Generally, while SPH feels that the DP law is a step in the right direction, it must be recognised that such a DP regime in Singapore is still in its infancy and has not yet reached the mature status of other leading jurisdictions. If Singapore is to achieve its status as a regional or global business hub, its organisations must be allowed to expand and compete with foreign organisations on a level-playing field. Local companies must be allowed to grow and increase their regional and global profile. This is especially since many foreign entities in the region operate in jurisdictions where there is minimal regulatory constraint.

84. This is especially so as advancement in technology and the increasing use of the internet as a medium for delivery of services and content have resulted in increased competition on the international stage. As the reach is broadening, more competition is generated across territorial boundaries and local companies have to compete on the global stage.

85. Therefore, in reviewing the comments received from this public consultation, MICA must be mindful not to create an overly regulated environment. Over-regulation will unnecessarily constrain local organisations and increase compliance cost, resulting in decreased competitiveness among local companies *vis-à-vis* their foreign counterparts.

86. SPH looks forward to future involvement in the public consultation process.

87. Please do not hesitate to contact the undersigned (Email: limmlg@sph.com.sg) if you have any queries or require any clarification.

Yours faithfully

Ginney Lim May Ling (Ms)

General Counsel,
Executive Vice President,
Corporate Communications &
Group Company Secretary