BT's Response to the Public Consultation of the Proposed Consumer Data Protection Regime for Singapore

25 October 2011

For further information, please contact:

Stella Teng Lih Ling

Senior Regulatory Advisor

BT Singapore Pte Ltd

Office: (65) 62907262

Mob: (65) 82233165

stella.teng@bt.com

Introduction

BT thanks the Ministry of Information, Communications and the Arts ("MICA") for the opportunity to contribute our views on the proposed consumer data protection regime for Singapore (the proposed new DP regime).

BT is one of the world's leading communications services companies, serving the needs of customers in the UK and in more than 170 countries worldwide. Globally, we supply managed networked IT services to multinational corporations, domestic businesses and national and local government organisations. We have adopted an industry sector-based structure to address customer needs in four global sectors, namely, Banking and Financial Markets; Commerce; Consumer Packaged Goods; and Government and Health.

BT has a strong interest in Singapore, being present in Singapore via its wholly owned subsidiary BT Singapore Pte Ltd (BT Singapore), the regional HQ for South East Asia, one of the largest foreign IT networked service providers in Singapore and the region. BT Singapore is a fully licensed telecommunications operator in Singapore with a Facilities-Based Operator (FBO) Licence.

We recognise that the subject of data protection (DP) has become increasingly important for global policy makers from the ongoing and varied states of debate across the globe. BT with global footprints and whose home market is widely recognised as one of the world's most competitive, have shared with global policy makers our views on DP.

Executive Summary

BT welcomes and supports the introduction of a general DP framework in Singapore, which is light-handed in nature with a focus on the objectives of protecting consumer/public interest as well as facilitating economic interest.

We believe that the proposed new DP regime will play a critical role in creating certainty and clarity for our operations in terms of planning and delivering our services to corporate customers in region.

We have restricted our comments to what we believe are the following key areas in response to the specific questions raised by MICA.

- Role and accountability of data controllers versus data processors
- Personal data definition and exclusions
- Cloud computing and the potential issues with regard to DP – to ensure that the impacted industry sectors are able to comply with the proposed new regime meaningfully and that the compliance costs are reasonable

- Data Protection Commission (DPC) set-up – structure and power, role and function, dispute resolution and appeal procedure, service provider's obligation to register with and provide regular reports to DPC
- Alignment of existing sectoral DP framework with the proposed new regime
- Consistency with recognised DP regimes worldwide and FTAs consideration
- Jurisdictional reach
- Data transfer
- Appropriate penalty and enforcement regime
- Do-Not-Call (DNC) registry – scope and compliance costs
- Regulations, codes of practice, guidelines, exemption orders, transitional arrangements

Views Regarding Specific Questions raised in the Public Consultation Paper

1. **Do you have any views / comments on the impact of the proposed DP law on specific sectors? Do you have any suggestions on measures to mitigate this or any other anticipated impact?**

- It is indicated in paragraphs 3.28 and 3.29 that an organisation that is merely in the business of processing personal data on an outsourced basis is not excluded from the proposed new regime, where such an organisation is likely to be deemed to have control over the personal data.
- BT does not think that "data processors" should be required to comply with this proposed new regime. While it is normal for "data controllers" to be subject to regulations about how they should collect and use personal data, it is unusual for "data processors" to be so. This is because normally a "data processor" simply acts under the direction of "data controller" and most jurisdictions take view that "data controllers" are the most suitable party to have the obligations of complying with the law as to how they collect and use data. In practice a "data processor" will take data supplied by or collect on behalf of a "data controller" and provide services to the "data controller" relating to such data. As an outsourcing service provider, BT needs its corporate customers to ensure that they have all the necessary consents from their end-user customers for the activities they are outsourcing to us to perform.
- We would encourage MICA to consider (i) the way in which globalised ICT service providers (including telecoms operators who provide outsourcing and professional security services) operate and (ii) the increasing interest and development in cloud computing solutions. Corporate customers may have many sites around the globe served by either a single service provider, or, in some cases, by more than one

service provider over the relevant service provider's own platform or third party service provider's platform. The single service provider or the principal service provider may then need to transfer and consolidate databases, change and transform the mode of service delivery for back-up and disaster recovery purposes. The question would be which country's DP regime would apply and who has the accountability to comply with it. In this regard, we think that it would be most practical to subject the "data controller" (being the corporate customer, who owns the contractual relationships with their end-user customers, being the data owners) to the relevant DP regime(s) applicable in the country(ies) where the data collection is conducted and where the data collected is sourced from. The "data processor" would be contractually liable under the obligations contained in the outsourcing contract agreed with the "data controller". We are concerned that the currently proposed more onerous approach of placing the legal obligations on the "data processor" will unnecessarily hinder business in Singapore and affect Singapore's reputation as a place to do business without unnecessary restrictions.

2. With reference to paragraph 3.8, do you have any views / comments on the concurrent application of the DP law with existing sectoral regulations?

- Concurrent application of the DP law with existing sectoral regulations will need to be considered thoroughly and the sectoral regulations and the DP law should be aligned before implementation so that those businesses which are impacted by the proposed new regime are clear as to their specific obligations under their sectoral licences/regulations and/or the DP law.
- BT favours approaches to data protection that are focused on measures that actually protect the personal privacy of individuals and not prescriptive regimes that are focused on form and procedure.
- There should be consideration and guidelines provided in circumstances where there may be conflict between the DP law and existing sectoral regulations, or in the event of situation where both the DP law and existing sectoral regulations cover the same scope but with varied penalties or enforcement regimes.
- It is indicated in paragraph 3.8 that sectoral regulators may apply to the DPC to exempt their licensees from specific requirements under the DP law where necessary. Does that mean sectoral licensees will be consulted by their sectoral regulators to assess whether there is any specific requirement under the DP law which may be considered for exemption application to DPC, before the DP law comes into effect? For practical and compliance costs reasons, sectoral licensees may require the opportunity to seek clarification from their respective sectoral regulators and/or the DPC (via sectoral regulators or direct from the DPC?) on

the rationale of being subject to compliance obligations additional to their existing sectoral obligations and to explore possibility of obtaining exemption from the DPC via their respective sectoral regulators.

3. Do you have any views / comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?

- BT considers that the personal data definition should be more clearly defined without being prescriptive, i.e. information which relates to a living person who can be identified from that data alone or from that data and other information which is in the possession of the data controller, and relates to that living person.
- MICA has identified two main categories of personal data, i.e. data with unique identifiers and data about an identifiable individual (with the example of an individual's mobile phone number which can be considered as personal data if the individual is identifiable through his phone number). In our advanced technology and social networking society, there are many other examples of data about an identifiable individual such as email address, social network user ID, etc.
- We support the proposal that DPC will publish guidelines following the enactment of the DP law to provide greater clarity to organisations by giving examples of information that may constitute personal data. For practical and compliance costs reasons, we believe that the guidelines should be published by DPC as early as possible to provide businesses which may be required to comply with the DP law adequate time to prepare before the DP law becomes effective. We would recommend that the DPC collaborates with sectoral regulators in consultation with the sectoral licensees/public to develop the guidelines. The establishment of the DPC is therefore one of the priorities leading to the implementation of the DP law.
- From an ICT and Telecommunications service provider perspective, organisations who provide outsourcing services, as well as telecommunications services may collect and process the following types of data as a "data controller" and/or "data processor":
    - data relating to end-user customers or employees of corporate customers collected and processed on behalf of corporate customers as part of operational requirements and/or sectoral licence obligations, e.g. call logs, call media from conference/video call recordings, network monitoring reports, email and internet usage logs, remote access logs, etc;
    - data relating to corporate customers and their employees/agents collected and processed as part of operational requirements as a telecoms service provider and/or sectoral licence obligations, e.g. we may keep certain data relating to corporate customers and their employees/agents in our systems

which may be used for operational purposes as well as for data retention obligation purposes; and
    - employee data.
- We consider it unusual that the current proposed "personal data" definition covers any data about an "identifiable individual". In most jurisdictions the definition would normally be limited to only data from which the "data controller" could identify the individual using the other information in his possession. Otherwise with the currently proposed definition certain data in the possession of a "data controller" could amount to personal data (and therefore be covered by the DP law) simply because somebody else could identify the person from the information. We would recommend applying a narrower scope of definition to avoid confusion and to prevent a business from having unexpectedly wide compliance obligations under the DP law.
- Included in the definition are unique identifiers such as national registration identity card numbers, passport numbers and photographs, and mobile phone numbers. We would ask for clarity as regards the processing of unique identifiers where other data necessary to identify an individual is not present – for instance, identification would not be possible if all that was present was a list of passport numbers. Would these things be considered personal data if the entity processing them had no ability to cross-reference the data with other data – for example, if all that was being provided was the network across which mobile phone data travels?
- We would agree with the exclusion of business contact information and product information.
    - We suggest that the new legislation use the Work Product Information definition from the British Columbia Personal Information Protection Act: *"work product information is information prepared or collected by an individual/group of individuals as a part of the individual's/group's responsibilities or activities related to the individual's/group's employment or business, but does not include personal data about an individual who did not prepare or collect the personal data"*
    - These exclusions don't exist in most countries but are sensible – and would mean that a person's name as the author of a report, or the sender or receiver of a work email, would not be considered to be personal data, and as such would not fall within scope of the DP law. This may seem minor but it is very problematic in the UK where this exclusion doesn't exist especially as regards data subject access requests where it is necessary to redact the names of all the individuals other than the data subject.

4. **With reference to paragraphs 3.15 to 3.16, do you have any views/ comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views / comments on the proposed approach to the protection of personal data of the deceased?**

- We are of the view that the new DP law should not apply to deceased people. DP laws are supposed to protect living individuals only and its extension to dead people creates a more onerous regime with higher business compliance costs and with little real benefit. The majority of data protection regimes only protect living people.
- We believe it is problematic for data concerning deceased individuals to be subject to the same general protection as all personal data for 20 years.
- As regards the narrower exception mentioned at 3.16 whereby data about deceased individuals would only be protected in relation to unlawful disclosure, this is a more manageable approach than the broad applicability of data protection laws to deceased individuals.
- We would recommend that there should be no restriction on organisations deleting data about deceased individuals, unless there is a legal or some other compelling reason to retain the data. Regulation relating to this may need to be reviewed in consideration of data retention obligations which may require certain data kept to be deleted upon the expiry of the time period required for data retention.

5. **Do you have any views / comments on the proposed organisations covered by the DP law?**

- Generally this is in line with most major DP regimes worldwide.
- In relation to the exclusion of the public sector from the DP law, MICA indicated that the public sector is governed by its internal data protection rules and regulations and that the public sector DP framework is consistent with the principles of the Model Code similar to the proposed new regime, with certain differences due to the specific needs of the public sector. We note MICA's proposal to exclude from the DP law personal data in the custody of a person acting as an agent of the public agency. We would seek MICA's clarification on the circumstances in which an organisation may be considered to be acting as an agent of the public agency. Would private sector organisations providing services to the public sector be subject to the DP law or the public sector DP framework?
- There should be consideration of and guidelines should be provided on circumstances where there may be conflict between the DP law and the public sector DP framework, or in the event of situation where both the DP law and the

public sector DP framework cover the same scope but with different compliance obligations or penalties or enforcement regimes.

6. **With reference to paragraphs 3.20 to 3.22, do you have any views / comments as to whether the DP law should extend to organisations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore? Do you have any suggestions as to how the DP law could be implemented if it should apply to such organisations?**

- Extra-territorial reach is a challenging issue to address but for deterrent purposes we think that the DP law should apply to all organisations collecting and processing data in Singapore. MICA and the DPC will need to consider thoroughly about how it would monitor, ensure compliance, and enforce the legislation in the event of dealing with organisations outside of Singapore.
- For practical reasons, BT would recommend that if an organisation complies with the DP law in its country of origin which is of the same and/or more onerous, then such organisation may be deemed as in compliance with the Singapore DP law. In assisting organisations with clarity on this, we would suggest to have a non-exhaustive list of countries that the MICA and the DPC consider to have a sufficient level of DP law in existence to meet this compliance level which is accompanied by the principles of DP law that must be met for compliance to be deemed.
- Further, in consideration of globalisation, we would also strongly suggest that MICA considers the possibility of including with the DP laws some form of group company exclusion allowance to enable global organisation such as BT to work efficiently and effectively within its own group environment. We would suggest that this be of considerable importance to all global companies and within the spirit in which the Singapore DP law is being created.
- MICA may want to consider including data protection in bilateral/unilateral discussions with other jurisdictions to facilitate the implementation and alignment of DP regimes across different countries.

7. **Do you have any views / comments on the proposed general exclusions from the DP law?**

- Please see comments to Question 5 above, which also relate to the general exclusions.
- We note and support the proposed exclusion for business contact information, which refers to information to enable an individual to be contacted in relation to

their employment, business or profession, e.g. name, position name, title, business telephone number, address, email or fax number of the individual.

- We request MICA to amend the definition of "business contact information" to indicate that business telephone number may also include mobile phone numbers in consideration that for work purposes employees are usually nowadays provided with both a desk phone number and a mobile phone number.

8. **With reference to paragraph 3.26, do you have any views / comments as to whether there should be exclusions for artistic and literary purposes under the DP Act? How should these exclusions be defined if exclusions for artistic and literary purposes should be provided for?**

- No comment.

9. **Are there any other exclusions that should be catered for under the DP Act?**

- With reference to paragraph 3.8, would this be related to the request for exemption from sectoral regulators? If yes, then as a FBO telecommunications licence provider, would we be required to seek exemption/exclusions from the IDA?
- As mentioned in our comments to Question 5 above, we suggest that exclusion be provided in relation to the collection, use or disclosure of personal data within a group of companies.
- We would suggest MICA and/or IDA consider the exemption/exclusion of managed network services from the DP law. There may be a scenario where employees of corporate customers in using corporate communications services may have the option to configure the service to block his/her user level phone number from being displayed when he/she makes a call. This request may be overridden in an emergency where in the event that a caller makes a call to access emergency services, the service provider will be obliged to override the user level phone number blocking to present the phone number (CLI) of such employee of the corporate customer to the local telecommunications service provider for onward transmission to the emergency services so that his/her whereabouts can be located.

10. Do you have any views / comments on the proposed general rules under the DP law?

- Lack of "data controller" and "data processor" distinction: The proposed new regime does not contain the same defined "data controller" and "data processor" distinctions that are present in DP regimes in the EU and elsewhere; rather it states that "organisations will be held responsible for personal data under its custody or control, including personal data that is not in the organisation's custody but is under its control".
    - In terms of application, this definition would effectively make "data processors" liable alongside "data controllers", as "data processors" are responsible for data in their custody. Under the EU legislation, only the "data controller" is liable to the DP authorities.
    - Generally, there are issues with the controller-processor distinction in the modern world as it's often difficult to determine who is actually in control of the data (for example in many cloud computing solutions).
    - However, in the context of BT's role as a global network service provider where we are primarily operating as a "data processor" on behalf of our corporate customers, the EU approach, whereby the "data controller" is solely liable, is preferable. We are mere data processors who have no ability to obtain consents or interact with a data subject.
    - Many of the corporate customers BT deals with are global organisations; they will be used to the "data controller-data processor" construct and complying with the proposed new regime that does not use this model will undoubtedly add complexity and compliance costs to their business.
    - We would also like to highlight the point that data flow in the modern technological environment is very fluid often involving multiple organisations as data processors. It would therefore be very difficult for the DPC to identify which organisations are liable for a particular data issue. With the "data controller-data processor" construct it is a straightforward approach for the DPC because the "data controller" is responsible for any issues that occur downstream.
- We support MICA's proposed contextual approach to consent.

11. With reference to paragraph 3.35, do you have any views / comments as to whether individuals should be deemed to have given consent for organisations to collect, use or disclose their personal data if they are notified and given reasonable time to opt out but do not?

- BT is supportive of the proposed opt-out approaches.

12. **Do you have any views / comments on the proposed rules on collection, use and disclosure of personal data?**

- No comment.

13. **Do you have any views / comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organisations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organisation? Are there any other exceptions that should be provided?**

- No comment.

14. **Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined at paragraphs 3.60 to 3.61?**

- We would suggest that the DPC considers developing a set of guidelines relating to the transfer of personal data outside of Singapore.
- While we recommend the principle that a "data controller" should have the obligation under the DP law to take steps to ensure locations outside of Singapore to which the data is transferred adequately protect it, the DPC needs to provide some guidance on what this will actually mean, i.e. a list of countries where this protection is currently present would be a useful starting point, or some principles as to how adequate protection is established.
- We also suggest including in the guidelines the definition and examples of what may be considered a transfer of personal data outside of Singapore. For example:
    - the transfer of data which may not be identifiable with an individual where the recipient of the data does not have the part of the data which in combination with the data transferred may be identifiable with the individual – whether this may be excluded from the proposed personal data transfer obligations.
    - if selected employees of the "data controller" and "data processor" are accessing personal data via a secure online portal from other countries would this be considered a data transfer activity?

15. Do you have any views / comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67?

- No comment.

16. With reference to paragraph 3.67, do you have any views / comments as to whether organisations should be required to specify the retention period when collecting personal data?

- We would not recommend having a specified retention period since this will restrict how long data is stored even if it continues to be required beyond the permitted retention period. This would be a difficult situation for businesses in Singapore.
- There are likely to be different retention periods required depending on the type of data due to legal and tax requirements.

17. Do you have any views / comments on the proposed rules on access to and correction of personal data?

- We would be supportive of a soft approach to dealing with request within an appropriate timeframe, where a minimum of 40 days would be in line with the practice in other jurisdictions.
- With reference to paragraph 3.73, we are supportive of the circumstances where organisations may refuse to deal with a request. However, we would seek a more explicit position on the requirement for requests to be reasonable and proportionate, as well as specific in terms of the actual data being requested.

18. Do you have any views / comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?

- It's important that enforcement powers are not immediately enforced in a "draconian" way as this could discourage organisations from doing business in Singapore.

19. Do you have any views / comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views / comments on the criteria for breaches that would warrant financial penalties?

- This section discussed the proposed "tiered" penalty regime which will enable the DPC to enforce penalties commensurate with the seriousness of any violation. We are concerned that it is not indicated how and who will determine the "seriousness" of a violation. In this respect, we would suggest that a clear statement as to the type of violation and level of penalty should be included. In addition, in consideration of ensuring compliance and keeping with the spirit in which this law is being created, we would encourage a more pragmatic and less litigious approach to enforcement and compliance by organisations and individuals. With this in mind we would suggest adopting an approach of collaboration and communication with the DPC prior to any consideration to prosecution is given. We would suggest that this could include steps such as, correction or enforcement notices, informal meetings with training, recommendations and guidance, and moving forward to arbitration or mediation on alleged disputes. With, as a last resort, prosecution for non-compliance.
- Further, we note that it is proposed that the DP law (i) allows the DPC to impose a financial penalty taking into account the level of damage to a person, and (ii) allows an individual to seek separate redress through civil proceedings. Our view is that both options should not be made available at the same time, as this could lead to a double penalty on the organisation, which we suggest is unjust. We would suggest MICA considers amending the financial penalty to exclude any consideration of the level of damage to a person but to allow the DPC to make a separate recommendation for damages payable to an individual, but such recommendation be non-binding on the parties.
- We reference to paragraph 4.4 which proposed that the DPC will have powers to issue orders for an organisation to rectify non-compliance with the DP law, and require the organisation to pay, within specified period, a financial penalty of such amount not exceeding $1million. We support the proposal that in the event a particular incident constitutes a breach of both the DP law and other sectoral regulation, it is preferable that the organisation be subject to the investigative and enforcement actions of one regulator. However it is not clear how this will be decided. Even though the breach may be concurrent within two DP regimes, the remedies and penalties may vary. Would it be the case where in the event of concurrent breach, the DPC will as a default, refer the incident to the relevant sectoral regulator?
- Would there be similar appeal channels within the sectoral DP frameworks with the proposed appeal channels under the DP law indicated in paragraph 4.6? For

instance will an independent Appeals Board hear appeals against the DPC's decisions? The Appeals Board's decisions could be brought to court for appeal or review, and individuals could separately seek redress via civil proceedings in court.

- We note and support the proposal from paragraph 3.5 that the DPC would investigate cases of non-compliance based on complaints where a complaints-based approach rather than a more stringent audit-based regime is adopted. We also support the proposed circumstances in which the DPC may refuse to conduct or continue investigations or review.

20. Do you have any suggestions on specific guidelines that the DPC should provide to help organisations achieve compliance with the DP law?

- It is proposed that guidelines on the following are developed by the DPC in consultation with the relevant sectoral regulators and licensees. This would help organisations comply with the DP law in a cost-efficient way:
    - personal data – definition and exclusions
    - consent
    - data controller-data processor distinction
    - jurisdiction reach and data transfer
    - existing data – scope of exemption
    - National DNC Registry – scope of telemarketing activities
    - DP law and sectoral regulations – single/concurrent compliance and exemptions

21. With reference to paragraphs 4.11 to 4.14, do you have any views / comments as to whether a one to two year "sunrise" period would be appropriate?

- We are supportive of a sunrise period. However, we believe that the estimate of a one to two year sunrise period may not be practical before the DPC is set-up and begins to perform some of its key roles and functions. As mentioned earlier, there are many implementation issues which will need to be thought out thoroughly, the DPC to be established, regulations and guidelines to be developed and published by the DPC with consultation with the relevant sectoral regulators and sectoral licensees, etc.

22. With reference to paragraphs 4.15 to 4.19, do you have any views / comments on the proposed treatment of existing personal data?

- No comment.

23. Are there certain organisations that may require different transitional arrangements?

- No comment.

24. Do you have any views / comments as to whether a National Do-Not-Call registry should be set up in Singapore?

- We note that the proposed DNC registry does not cover email addresses. We find this a strange gap in the current legislative proposal since it would seem to permit unsolicited electronic messaging using email. Given the current importance of email in business most jurisdictions choose to regulate both personal data use and unsolicited electronic messaging.

We thank MICA for its attention to our response and are happy to answer any queries it may have on the above.