Trust Bank Singapore Limited
Registration No. 202039712G
77 Robinson Road
#25-00 Robinson 77
Singapore 068896
trustbank.sg

PDPC's Public Consultation on the Proposed Advisory Guidelines on Children's Data

We enclose our comments to questions outlined in Part II of the above consultation paper for your consideration.

For clarifications, you may contact the following parties:

1) Paul Chung, Chief Compliance Officer and Data Protection Officer
   Email: paul.chung@trustbank.sg

2) Jennifer Tan, Regulatory Compliance Lead
   Email: jennifer.tan@trustbank.sg

Thank you.

Questions	Comments
Question 1: What are your views on the proposed scope of application of the Advisory Guidelines: a. to organisations that offer products or services that are likely to be accessed by children, or are in fact accessed by children, even if the products or services are not targeted at children; and b. that the requirements relating to the protection of children's personal data within the Advisory Guidelines will apply to organisations that are data intermediaries?	We are of the view that the proposed Advisory Guidelines should be applicable to both organisations (DC) and data intermediaries (DI) which handle children's personal data, but only as relevant to the roles of a DC and a DI. In this regard, if there are additional protections required, these should apply to both DC and DI. However, if additional rules apply to obtaining consent, these should only apply to DC.
Question 2: Section 18 of the PDPA provides that an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances. What are examples of reasonable purposes for organisations to collect, use, or disclose children's personal data?	Organisations such as banks would likely collect, use or disclose children's personal data, for the purpose of providing savings accounts and other products such as insurance (i.e. travel insurance, endowment plan for child's education). However, we do not think the Advisory Guidelines need to be prescriptive on listing out the reasonable purposes.
Question 3: When communicating with children, organisations must use language that is readily understandable by children, and can use visual and audio aids to support the child's understanding. What in your view are examples of such communication with children?	While we have in general simplified the language used in our existing product disclosure documents with our customers, we might need to complement these with additional educational aids to explain to this customer segment who are children aged 13-17. Examples can be videos on how a savings account works, the payment functions/modes available and how to protect their accounts and report unauthorised transactions. These topics can also be in other forms such as a "cheat sheet", cartoons, info-graphics, flow charts, diagrams, maps, etc. However, this should all only be as needed in order to be reasonable in each context. We respectfully request that the guidelines should not be prescriptive on this point. The key principle should be that organisations need to communicate

	with children in a clear way so that they can understand. This will also depend on the age group the organisation is working with. There could be variation in level of understanding/maturity from the younger to the older end of the age group we are concerned with here (e.g. a 17 year old will understand a lot more than a 13 year old). Alternatively, the parent/guardian could be involved to support the child's understanding, given that the children in this age group may be less aware of the risks of sharing data with organisations and the above education aids cannot adequately mitigate the risks.
Question 4: How should organisations minimise the collection, use, and disclosure of children's personal data? a. If an organisation were to collect personal data in order to ascertain their users' age, what measures or best practices should an organisation be undertaking? b. If an organisation were to collect geolocation data, should geolocation be switched off by default so that products and services cannot automatically start collecting geolocation data when they are first used?	For organisations such as banks, we collect date of birth as part of our customer due diligence. For geolocation data, this could potentially be used for fraud monitoring e.g. customer is in Singapore but transactions are being initiated from overseas. Having the geolocation on will also help reduce the impact of fraudulent transactions and facilitate in providing prompt responses and actions. We are of the view that the proposed Advisory Guidelines need not be prescriptive on more specific data minimisation rules that need to apply to children's data. The data minimisation principle is general and overarching that organisations should not collect excessive personal data and there is no need to set out prescriptive rules specific for children's data.
Question 5: What are examples of situations where an organisation should conduct a Data Protection Impact Assessment (DPIA) before releasing products or services likely to be accessed by children? What should an organisation consider when conducting such a DPIA?	Nil
Question 6: The PDPC notes that the age threshold of 13 years appears to be a significant one in relation to the protection of minors, and moving forward is considering to adopt the practical view that a child that is between 13 and 17 years of age will have sufficient understanding to be able to consent on his or her own behalf to the collection, use, or disclosure of his or her personal data, as well as withdraw such consent. What are your views of when a child can give valid consent on his or her own behalf under the PDPA?	We note that the PDPC has proposed to adopt a practical view that a child between 13 and 17 years of age can give a valid consent. However, the Civil Law Act sets the age of majority to enter contracts in Singapore as 18. Given the conflict between the Civil Law and the proposed Guideline, we anticipate issues pertaining to legal enforceability. On one hand, the PDPC is saying that children can give valid consent, however the Civil Law Act says that contracts with minors cannot be enforced. The PDPC should consider how these points interact.

trust

Question 7: The PDPC has said that children's personal data is of a more sensitive nature, and that organisations are required to take extra precautions and ensure higher standards of protection under the PDPA with regard to such data. The PDPC is considering making it a best practice for organisations handling children's personal data, to implement both the Basic and Enhanced Practices listed in the Guide to Data Protection Practices for ICT systems. Are the practices listed in this Guide adequate? Are there additional measures that organisations should undertake for the protection of children's data?	For organisations such as banks, there are sectoral guidelines i.e. MAS' Technology Risk Management Guidelines which banks are expected to comply with. The information protection control objectives for systems in both the MAS' Technology Risk Management Guidelines and Basic and Enhanced Practices listed in the Guide to Data Protection Practices for ICT systems are principally aligned. Hence, from the perspective of banks, this should be considered adequate where technical controls are concerned for protection of children's personal data.
Question 8: The PDPC requires an organisation to notify each individual affected by a notifiable data breach in any manner that is reasonable in the circumstances. A notifiable data breach is a data breach that (a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale. Where a notifiable data breach occurs, under what circumstances do you think it would be prudent for the organisation to inform the child's parent or guardian of the breach, considering that this would allow the parent or guardian to take steps to mitigate the harm to the child of the breach?	We propose that the parent or guardian be informed only in circumstance where the data breach could result in significant harm to the child and only if parental consent was required when the initial collection happened. In the case of a bank, if we allow minors to apply for a bank account in their own name, without parental consent, then we are of the view that the parent or guardian does not need to be informed of a breach (which could be at odds with banking confidentiality rules). However, if a bank requires parental consent for customers below a certain age or a parent must apply together with very young child for certain kinds of accounts, then the parents should be informed of a notifiable data breach that is likely to result in significant harm to the child.