Public Consultation for Proposed Advisory Guidelines on the PDPA for Children's Personal Data

Date

31 August 2023

Name of Organisation

Standard Chartered Bank (Singapore) Limited

Contact Person

Seow Jen Yi
Data Protection Officer
Singapore.Privacy@sc.com

Standard Chartered Bank (Singapore) Limited ("SCB") welcomes the opportunity to provide our feedback on the proposed Advisory Guidelines on Personal Data Protection Act for Children's Personal Data ("AG"). The Bank is generally supportive of the issuance of guidance with regards to handling of children's personal data, as well as to accord higher standards of protection to children's personal data where appropriate.

Q1: What are your views on the proposed scope of application of the AG:

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?**

Response:

a. The Bank is supportive of the scoping of the AG to apply to offering of products / services that are likely to be accessed by children, or are in fact accessed by children, which allows for a proportionate approach in applying the AG, that enhances the protection of children's personal data without introducing overly onerous expectations to organisations where there is minimal privacy risk in relation to children. For avoidance of doubt, the Bank's understanding is that the AG is not intended to be applied if the product / service does not require collection, use or disclosure of children's personal data, regardless of whether it is likely to be accessed by children. For example, if a mobile application is downloaded by an adult (where only an adult's personal data was collected), but is subsequently accessed by a child, the organisation is not expected to apply the AG if there is no further collect, use or disclose any children's personal data.

In determining if a product or service is likely to be accessed by children, we respectfully suggest that the burden of determining such likelihood is left to organisations, as part of their internal assessments prior to launching the product / service. We also suggest that such assessment is based on a reasonableness approach.

As for products / services that are in fact accessed by children, we would like to clarify if this suggests an expectation for organisations to monitor the age of the users after launching a product / service, to assess if there is indeed access by children. This may be onerous on organisations, and there would need to be a means of tracking or estimating a user's age, which may involve collecting more personal data than what was initially required by the organisation.

The Bank would like to highlight that there should ideally be a differentiation in scenarios where the collection, use or disclosure of children's personal data is incidental, where the organisation is mainly dealing with a minor's parent or guardian. In such scenarios, the consent and notification to the minor's parent or guardian should suffice, rather than requiring a separate consent and notification to the child. Instead, it would be appropriate for the minor's parent / guardian to convey the necessary information to the child.

b. The Bank is of the view that the AG should apply to data intermediaries when processing children's personal data on behalf of an organisation, in line with the respective data protection provision in the PDPA that applies to data intermediaries.

Q2: 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?

Response:

Generally, the principles of Section 18 for determining reasonableness for collection, use and disclosure of personal data will still be relevant and applicable to the collection, use or disclosure of children's personal data. For avoidance of doubt, the measure of reasonableness should continue to be whether a reasonable adult (not minor) would consider the purpose appropriate in the circumstances.

A general rule of thumb is where the collection, use or disclosure of children's personal data is for purpose to consume product or services offered to them as target consumers without causing harm or violation of safety and/or law.

Examples of collection of children's personal data are registration of junior book club, opening of a junior saving account, registration for tuition services.

Q3: 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?

Response:

Such communications with children should be in clear and concise manner that is easily understood. Visual / audio aids or learning games may be considered to supplement the understanding of more complex concepts and may be more effective in engaging this demographic.

In such communications, we respectfully suggest a focus on clarity rather than comprehensiveness, where such simplified communications should convey key concepts, instead of being considered as a replacement of legalistic texts.

This will also aid in educating children on the concept of privacy and the potential impacts of the collection, use and disclosure of their personal data.

Further, we propose a differentiated approach, where such age-appropriate communications should be specifically applied to products and services that target children, and exclude such an expectation for products / services that incidentally collect children's personal data.

Q4: 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?**

Response:

a. Instead of a one-size-fits all approach, organisations should consider the types and amount of personal data that is already being collected for the purpose of the specific product and service that is being offered. For example, in the context of financial institutions, if date of birth is already being collected along with documentary evidence as part of the customer due diligence process, these organisations can easily use these personal data fields to ascertain a user's age without having to collect further information.

In contrast, if an organisation offers a product / service that does not collect any personal data that allow the deduction of the user / consumer's age, an assessment should be performed to ensure that a balance is achieved between data minimisation during the collection of additional personal data fields and the benefits of the age assurance.

b. Fundamentally, organisations should ensure that consent of the individual is obtained prior to the collection, use and disclosure of personal data, unless exceptions apply. The same concept should be applied to the collection, use and disclosure of geolocation data.

Q5: What are examples of situations where an organisation should conduct a DPIA before releasing products or services likely to be accessed by children. What should an organisation consider when conducting such a DPIA?

Response:

A DPIA should always be performed before release products or services that are targeted at children.

However, if a product / service is not targeted at children, but may incidentally be accessed by children, an organisation should assess how likely children will be accessing the product / service before determining if it will likely involve processing personal data of children. In the event that it is assessed that there is a high likelihood for children to access the product / service, a DPIA should be performed prior to release.

When conducting such DPIA, the considerations as per any DPIA should generally continue to apply and may expand to include other additional factors, such as ethical considerations of data usage and an assessment of intended and unintended outcomes, bearing in mind the child may lack the maturity and understanding. However, there may be a need for further guidance on how such considerations can be incorporated into a DPIA, and it will be good if the Commission can provide such guidance in the AG.

Q6: 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.

Response:

We are mindful that a typical 13-year-old child and a 17-year-old child may have a significant difference in the level of maturity and understanding in relation to the consent they are giving in relation to their personal data.

Children of 13 to 15 years of age may not have the necessary maturity and understanding to discern the consent they are giving or withdrawing.

We respectfully suggest that the Commission considers only treating children who are 16 years old and above to be of an adequate age to provide or withdraw consent on their own behalf to the collection, use or disclosure of their personal data. This would be aligned with the Children and Young Persons Act, where a "child" and "young person" are defined as one below 14 years old and one between 14 and 16 years old respectively.

Q7: 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?

Response:

Basic and Enhanced Practices as set out in the Guide to Data Protection Practices for ICT systems are adequate and should already be in line with industry best practices.

Q8: 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?

Response:

Generally, the prescribed data set out in the Advisory Guidelines on Key Concepts in the PDPA already considers scenarios where they may potentially be significant harm where children are impacted by data breaches.

For data breach notification on significant scale, we are of the opinion that the existing requirements suffice and there is no need for specific guidance in relation to children's personal data, given that the intent of this limb seems to be for identifying incidents of a systemic nature, regardless of the sensitivity of data involved.

We appreciate if the Commission can provide examples of steps parent / guardian can take to mitigate the harm to the child in the event of a data breach.

==End==