SUBMISSION OF COMMENTS TO PDPC'S PUBLIC CONSULTATION FOR PROPOSED ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR CHILDREN'S PERSONAL DATA

Submitted By: SGTech

Submission Date: 31 August 2023

Contact Information:

- Name: (Ms.) Sukaasini Latch
- Designation: Manager, Government Affairs & Transformation
- Email address: sukaa@sgtech.org.sg
- Address: 79 Ayer Rajah Crescent #02-05 Singapore 139955

Summary

In an age dominated by digital technology, the protection of children's data and privacy has become an issue of paramount importance. Children are increasingly active online, engaging with various digital platforms and services, and consequently generating vast amounts of personal data. In that regard, SGTech is supportive of PDPC's efforts to accord higher standards of protection to children's data through the proposed Advisory Guidelines to better safeguard children's data and privacy, by guiding organisations with key principles to uphold in their endeavors.

Children, being a vulnerable demographic, are particularly susceptible to the potential risks associated with data misuse and privacy breaches. Ensuring the protection of their data and privacy is not only a moral and ethical imperative but also a legal one. In this digital era, the consequences of failing to safeguard children's information can be profound and long-lasting, impacting their psychological, emotional, and even physical well-being.

Moreover, instilling a sense of trust in digital technologies from an early age is crucial for their healthy development and participation in the digital society of the future. Therefore, regulators and businesses must recognize the importance of robust safeguards for children's data and privacy.

We note that the proposed Advisory Guidelines are premised on the basis that unless parental or guardian consent is obtained, children's personal data should not be collected, used, or processed. This is very much in line with privacy legislations governing children's data worldwide, such as the Children's Online Privacy Protection Rule (COPPA) and the General Data Protection Regulation (GDPR).

SGTech's views and comments on the specific public consultation questions can be found below. Our responses are guided by the following key principles:

i. **Informed Consent**: Obtaining clear and informed (opt-in) consent from parents or guardians before collecting any personal data from children. This consent should be easy to understand and easily accessible. There is also a need to strike a balance between being able to verify that the consent provided comes from the parent or guardian (i.e. an adult) without the verification process becoming too onerous or complex to organisations.

ii. **Data Minimization**: Collect only the data necessary for the intended purpose. Avoid collecting excessive or irrelevant information about children.
iii. **Transparency**: Communicate clearly and be upfront about data practices. Inform parents, guardians, and children about what data is being collected, why it's being collected, and how it will be used.
iv. **Education and Digital Literacy**: It is paramount to promote digital literacy and responsible online behavior among children. Offer resources and guidance to help them understand the importance of privacy and how to protect themselves online.

Safeguarding children's data and privacy is an ethical and legal responsibility that extends to both regulators and businesses. Upholding a set of commonly agreed upon principles not only ensures compliance with guidelines but also contributes to the well-being of the next generation, fostering a safer and more trustworthy digital environment for children to thrive in.

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

It is reasonable for the Advisory Guidelines to apply if the nature of the service is such that it is targeted at children.

For greater accountability, we need to ensure that organisations are not able to avoid the Advisory Guidelines by including clauses into their Terms & Conditions such as "Only individuals who are 18 years of age or older are allowed to or should access the service or website". As such, it might be worth for the Advisory Guidelines to encapsulate this point in terms of the application of the Advisory Guidelines with respect to the nature of the goods or services, and not in terms of specification based on age limit.

It may not be a reasonable expectation on organisations for the scope of application to include products or services that are "in fact accessed by children" if an organisation's products or services are accessed by a child out of curiosity, with no clear intent or interest. In this regard, we would suggest introducing the concept of "actual knowledge", i.e. from registration, sign-ups, or any other qualifiers that show that the data processor has actual knowledge that the user is under the age threshold.

We recommend that the Advisory Guidelines should apply in either of the following cases:

i. The product, service or content is appealing to young audiences.

While the content for children below 13 years of age may be more straightforward, content for teenagers (~13-18 years of age) can become increasingly grey. One potential solution could be to survey the audience and establish a limit on what is considered a youth audience, which is most commonly set at 30% of the total audience below the age threshold.

ii. Actual knowledge that the data subject is below the age threshold.

Examples of soliciting actual knowledge include an age gate (year and month of birth), sign-up/registration, user generated content revealing the age, user surveys, etc.

Even if the product/service/content is not targeted to a young audience, having actual knowledge of the data subjects based on the verification points mentioned above should then allow for the Advisory Guidelines to apply to organisations.

Given that most youth related data protection provisions are based on the above two principles, this could be a good compromise between protecting young audiences and allowing organisations to continue to operate with minimal impositions/restrictions.

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?

This depends on what the data intermediary is doing on behalf of its customer. Outlined below are two situational examples to demonstrate when the Advisory Guidelines could apply and when they may not.

Example 1: Personal data is provided by the customer to the data intermediary so that the data intermediary can provide its services – perhaps an employer engages a data intermediary to process employee health insurance claims, which includes claims in relation to an employee's children and in such a case, the Advisory Guidelines should not apply to the data intermediary.

Example 2: Personal data is provided by individuals, which may include children, so that the data intermediary may provide their services – a shopping mall or a retailer in a shopping mall engages a data intermediary to do everything necessary for the shopping mall / retailer to provide a loyalty programme. In such a case, the Advisory Guidelines should apply to the data intermediary. Otherwise, a retailer that, for e.g., is a toy shop could outsource its loyalty programme to a data intermediary with the intention of avoiding the Advisory Guidelines.

The foundational principle should be based on consent. In the case of children, parental or guardian consent needs to be obtained (in a valid and conscious manner) in order for children's data to be collected and processed. Hence, the Advisory Guidelines should apply to organisations that collect personal data from individuals, whether or not the organisation does so as a data intermediary.

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 should be able to collect personal data about children on a mandatory basis only to the extent that the personal data is necessary for provision of the service. For example, exact location data is necessary for the provision of a game such as Pokemon Go, but is not generally necessary for the provision of other services.

Whether organisations should be able to collect other personal data about children on an optional basis (for example, to enable an organisation to understand its users better and/or to profile them for marketing purposes) is of course a policy decision but one that we support

in the interests of innovation and the ability of businesses in Singapore to provide their services effectively and efficiently.

Fundamentally, it may be beneficial to introduce the concept of data minimization by default, where only necessary data to provide the service/content/product should be collected, and to be kept for the amount of time that it is necessary.

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?

These could include Terms of Use, Privacy Policies, etc. that are written in a manner in which that can be easily understood by young audiences. A good example would be the notices on Lego's website under the Kids Section.

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?

As a first principle, before collecting any other information from the individual, an organisation that targets its goods or services to children must first set out to ascertain the age of the data subject. If their age is below the threshold, parental or guardian's consent must be obtained.

There are several ways to request users' age. The guiding principle from the perspective of the organisation that is collecting the personal data has to be that the user does not perceive any disadvantage of being under the threshold (for example, does not perceive that they will not be able access the service or that they will experience different content). Accordingly, we support self-declaration.

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?

Firstly, deciding on whether geolocation should be switched off by default depends on the nature of the service, i.e., whether geolocation is necessary for provision of the service. And if geolocation is necessary for provision of the service, is it necessary to collect the general location (i.e., the data subject is in Singapore or this person is somewhere in East Coast today and somewhere in Jurong West tomorrow, etc.) or is their (close to) exact location necessary?

Second, even if the geolocation is switched off by default because it is not necessary in order to provide the service, it may be quite easy to give a general explanation about what is being asked for and therefore to convince a child to turn it on – either general or exact geolocation – without the child understanding the underlying and arguably risky implications of doing so.

Globally, under most youth privacy protection provisions, precise geolocation is considered personal information. Therefore, in the case of children, if general or exact geolocation is turned off by default because it is not necessary in order to provide the service, it should require parental or guardian's consent before being collected.

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?

Our view is that a DPIA should always be conducted when an organisation plans to offer new services or services that are amended in a non-minor way. While opinions may differ on this point where services are offered to adults, the requirement should always apply to all categories of personal data that are generally considered to be sensitive (as, for example, set out in the regulations made for the purpose of considering whether a data breach involves significant harm), including where services are offered to children.

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?

Except for a very simple example of a child that signs up for a catalogue or something similar, in practice, the context of getting consent is always related to entering a contract (through the acceptance of the terms of use).

In Singapore, individuals who are 18 years of age have contractual capacity except in relation to a very small set of circumstances, for example, buying real estate. Hence, it makes sense that individuals who are 18 or over, should be able to give consent.

From a practical standpoint however, an adult – parent or guardian – will need to be involved whenever a teenager under the age of 18 wants to acquire a service and we see it as unduly burdensome on organisations to decide that all prospective users of a necessarily arbitrary age may or may not be able to fathom the risks associated with giving away personal data that possibly ends up in the wrong hands due to a data breach or even a business disclosure by a platform. (We also note that any organisation that must make such a decision should do so only after undertaking a properly scoped DPIA.)

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?

We agree that higher standards of protection are needed to govern children's data that can be very sensitive given the vulnerable nature of the demographic. The practices listed are adequate. Before additional measures are considered or included, it would be best to consult

the industry accordingly to understand the need, impact and implications of further enhanced measures on both individuals and organisations.

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 believe that it should be a blanket requirement for the consenters (that is, parent or guardian) to be notified, in addition to the child.

However, a practical concern may arise: the organisation may not have the contact information of the consenter. Hence, in order to be able to notify the parent or guardian, where current processes do not include collecting the name and contact details of the consenter (together with a process for ensuring that they remain up to date) organisations will need to reconfigure their sign-up processes to include this requirement.

We see this as unduly burdensome for organisations in Singapore so suggest that the fallback should be that (1) the consenter is notified only where current processes include collecting (and keeping up-to-date) the consenter's name and contact details and (2) where an organisation chooses at any time to change its processes so that consenter name and contact details are collected at the outset (and kept up-to-date) the requirement for consenter notification should not be retrospective (in the sense of requiring the organisation to implement the new process to its already existing service users).