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

Submitted by: TotallyAwesome Singapore Pte. Ltd.

Address: 168 Robinson Road, #22-03 Capital Tower, Singapore 068912, www.totallyawesome.tv

Contact Person: Marcus Herrmann, COO and Chief Safety Officer
marcus@totallyawesome.tv, 8743 6023

Dear Sir or Madam,
In response to the PDPC's Public Consultation, we would like to share our comments on the Proposed Advisory Guidelines on the Personal Data Protection Act for Children's Personal Data.

Response Summary

TotallyAwesome welcomes the proposed Advisory Guidelines for Children's Personal Data. In recent years several children's personal data regulations have been implemented in Asia and we believe it cements Singapore's leading role in Asia to specifically protect the most vulnerable in our society yet provide clear guidance to organisations and foster a stable economic environment for businesses to thrive in.

We base our recommendations on the following principles:

- **Age Threshold**: Defining the age threshold at which a child can fully understand the dangers and threats associated with disclosing personal data. See question 6.
- **Informed Consent**: We believe it is important to obtain clear and informed consent from a parent or guardian for the collection and processing of a child's personal data. Ensure that consent processes are user-friendly and transparent.
- **Age Verification**: We believe it is important to find a balance between accurate age verification and businesses interests to provide a frictionless user experience. See question 4.a.
- **Data Minimisation**: We would like to encourage organisations to collect only the necessary data from children and avoid excessive data collection.
- **Privacy by Design**: We encourage the "privacy by design" principles into the development of products and services targeting children, ensuring that privacy considerations are part of the initial design phase.
- **Personal Data Definition:** Apart from the obvious (name, address, email, phone number etc.) we recommend including what under COPPA is called "persistent identifiers over time". Examples include Cookies, Device IDs, Advertising IDs etc. These identifiers are used by advertising networks to track and build exact profiles of users. In the case of children's data and data breaches these profiles can potentially be used to harm children. We also recommend including pictures, voice and video recordings as well as precise geolocation (see question 4.b.)
- **Education and Awareness**: We encourage government bodies to provide educational initiatives to raise awareness among children, parents, educators and businesses about online privacy risks and best practices.

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

Based on common practice and other privacy regulations, we recommend that the Advisory Guidelines should be applicable if:

1) The content, product or service is primarily appealing to children, for example: animation content on a catch-up TV platform like meWATCH, then it can be assumed that children are actually consuming this content; OR
2) There is actual knowledge that the data subject is a child, for example the data subject reveals their age during a signup for a competition or club, a survey etc.

In either of above cases no data should be collected unless there is parental/guardian's consent.

We do not recommend applying the Advisory Guidelines in all cases where the products/services/content are "in fact accessed by children". As an example, a website with legal case studies could be accessed by a child preparing a school assignment. In this case, it would be impractical for the website owner to verify each and every visitor whether they're above the age threshold or not. The content is clearly not appealing to children and the website owner has no actual knowledge that a child is accessing it.

However, on the flipside, it is not sufficient for business to state that the content/product/service is not intended for children, and children are not allowed to access it, example YouTube used to state that the service can only be used by 18 year olds and above. However, there are millions of videos that are appealing to children on the platform[1].

In practice, the concept under 1) is open to interpretation and there will be situations that are not clear cut. Under COPPA for example, if there are opposing opinions, it is the Federal Trade Commisssion or a court of law that finally interprets whether content/products/services are appealing to children. In Singapore this could be the PDPC.

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?

Our advice is that the Advisory Guidelines should apply to data intermediaries that process children's data. We recommend the same principles as under answer a) above apply: If the data originates from a product/service/content that is appealing to children or b) if there's actual knowledge that the data subject is a child, then the Advisory Guidelines apply. Parental/Guardian's consent can be obtained for the collection processing and transfer of a child's personal data at the point of collection.

[1] https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law

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?

Children's personal data should only be collected with Parental/Guardian's consent. We do not recommend any exception to the aforementioned apart if the child could be harmed, for example a social service storing data of child abuse victims.

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?

We recommend the use of understandable language when it comes to privacy notices. The most critical elements that are relevant to the child user have to be mentioned in an age appropriate and understandable language. We suggest the following sections (with examples of language):

Exactly what the online service's approach to data collection is

It's important for publishers to set out their data collection 'philosophy' in order to give context and comfort to the user.

For example: We'll never ask you for personal information, but our app needs to collect some data from the way you use it in order to work. We'll always tell you what we're collecting and why, and we'll do our best to keep your information safe. You can help by not sharing any personal information on the app!

Exactly what personal data is being collected

Within this section the types of data should be detailed, and explained in simple terms.

For example: We need to collect your email address and username to create your account, and information about your device so that we can make the app look great.

Why their personal data is being collected

The user should be able to identify the purpose of processing, whether it is required for the service to work, to improve features, or to deliver advertising, etc.

For example: We collect non-personal info to give you the best app ever, so it looks good, contains everything you love and we know how to help you with any bugs.

If and how their personal data may be shared with third parties

For example: If the police or government ask us to help stop or investigate a crime we may have to give them your username and internet address.

The rights of the user and how they can exercise them.

For example: You or your parent or guardian can look at, change, correct or delete any information about you on the app. Just ask your parent or guardian to contact us.
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[2].

[2] https://www.lego.com/en-us/kids/legal/privacy-policy-short

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?

We recommend implementing age gates only if

1) the content is potentially appealing to children and data needs to be collected. Then below the age threshold parental/guardian's consent can be obtained and above the threshold regular user consent can be obtained or
2) the service should not be used by a certain age group (eg. social media platforms, alcohol online sales etc.)

In both above cases the Advisory Guidelines should be applicable.

We recommend ascertaining the age before collecting any other information. If the age is below the threshold then the parental/guardian's consent should be obtained **before** collecting any other information about the child. A recent COPPA fine against Microsoft (Xbox) illustrates this process[3]

There are several ways to determine the user's age:

1) Self-declared: the easiest to implement – but also the easiest to circumvent. Generally there are more honest answers by asking for the month and year of birth rather than asking for the age.
2) Actual age verification, eg. proof with official ID. We believe that, for the most common data processing activities, any age verification technique that requires the collection of more personal data—such as a national ID card, or a national insurance number—is overly intrusive and impractical for organisations.
3) The future of age verification: based on automated, passive ways of detecting whether a user is likely a child or not, and providing that assessment, along with a confidence score. For example, collecting multiple signals from user behaviour (locally, on the device, without tracking or data collection) such as speed of typing, touch screen patterns, etc.

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?

We strongly recommend that precise Geolocation is considered personal information and thus a) should be turned off by default for child-directed content and services AND b) parental consent should be obtained before geolocation tracking can be turned on.

As an example, Pokemon Go necessitates precise geolocation to use the app. Before a child can sign up and use the app, parental consent is obtained[4].

[3] https://www.justice.gov/opa/pr/microsoft-agrees-pay-20-million-civil-penalty-alleged-violations-children-s-privacy-laws
[4] https://nianticlabs.com/parents?hl=en

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?

We recommend that a DPIA is conducted in any case whether the service is child-directed or not.

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?

Looking at other privacy regulations these are the age thresholds: COPPA <13 years old (to be revised to <16 years old), GDPR <16 years old, the revised AU Privacy Act will be either <16 years old or <18 years old, the Indian DPDP is setting the age at <18 years old.

Even with clear privacy notices, we believe that young people are not aware of the personal data that is routinely collected from them while they use digital services, whether the collection is passive (such as by advertising technologies) or active (such as games asking for permission to record location). These Data collections result in threats when data breaches occur.

Most importantly, paediatric psychologist advise[5] is that young people can only fully comprehend the concepts and the dangers associated with giving consent to personal data collection from the ages of 18 years old.

TotallyAwesome's recommendation is to protect Singapore Young people until the age of 18.

[5]Appendix 1 to this document: Amanda Abel, Paediatric Psychologist, on the age threshold for giving informed consent

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 children's personal data is of a more sensitive nature and should be protected at higher standards. While not 100% perfect, to be practical for Singaporean businesses, the Basic and Enhanced Practices are a good compromise.

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 recommend that the initial consent-giver should be notified. In the case of a child, it is the parent/guardian. The data collector can easily collect contact details of the parent/guardian at the point of consent granting.

Appendix 1: Advice from Amanda Abel (Paediatric Psychologist, BSocSc, BAppSc(Psych)(Hons), MAPS, MAAPi, MSPS) on the age threshold for giving informed consent

Friday 1st September 2023

"A young person has capacity to give consent when they have sufficient understanding and maturity to understand what is being proposed. They need to understand the consequences of giving or not giving consent and they need to make their decision based on reason – and have the ability to communicate this. Given the significant risks involved with data privacy, and the variation in executive functioning development in adolescents, making a decision based on reason could be a particularly challenging task and even more so when the circumstances around the situational effects of providing consent are considered. To expand on this, an individual is likely to be asked to provide consent as a prerequisite for accessing something motivating. It may be difficult for an individual with limited executive functioning capacity to balance these needs and make a decision on reason. For this reason we recommend parental consent is given for all individuals under 18 years of age.

Further, it is recommended that when parental consent is being obtained on behalf of a minor, that there is a verification process to confirm that this person has parental responsibility for the child and is the legally recognised person with decision-making rights. "

Appendix 2: About TotallyAwesome

TotallyAwesome is a Youth-first specialist marketing and media platform focused on connecting brands with youth in a safe, relevant, and effective way. We are driven to make a positive impact for our Youth in the digital world. At the heart of everything we do is Youth.

TotallyAwesome offers Youth-first, Youth-safe engagement across thousands of YouTube channels, apps, games, and websites. Our extensive research gives us a deep understanding of Gen Z and Gen Alpha, while our 'zero- data', contextual intelligence solutions enable safe digital engagement with a Youth audience. Our Youth-first curated and human moderated technology solutions reach more than 500 million active monthly users across Asia Pacific. From content creation to innovative gaming solutions, we bring excitement to the digital world of our Youth.

TotallyAwesome work with a team of qualified psychologists to provide evidence based insights, guidance and to inform our work to deliver a Youth-safe digital world for Youth.

All our products and services have been specifically designed for the compliance requirements of the youth market, including COPPA, GDPR, the Australian Privacy Act, the Indian DPDP Bill, the Korean PIPA, the Singapore PDPA, the Vietnam Privacy Decree, and all other privacy regulations.
In addition, our *Kidaware* education programme is used extensively by brands and agencies to train their employees in children's data privacy laws and advertising standards - we educated hundreds of digital media professionals across Asia Pacific.

Finally, we have been actively involved in working with the market and regulators in developing and implementing digital child safety policies, including the revision of the Australian Privacy Act.