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

TikTok Pte. Ltd.
One Raffles Quay, Level 26 South Tower
Singapore 048583

31 August 2023

I. Statement of Interest

1. This submission is in response to the invitation by the Personal Data Protection Commission ("**PDPC**") to provide feedback on the Proposed Advisory Guidelines on the Personal Data Protection Act for Children's Personal Data ("**Advisory Guidelines**"). TikTok Pte. Ltd. ("**TikTok**") is grateful for the opportunity to engage with PDPC on this topic of significant public interest and to provide our written feedback.

2. TikTok is the leading destination for short-form video. TikTok's mission is to inspire creativity and bring joy. We are building a global community where people can create and share, discover the world around them, and connect with others across the world. We are committed to maintaining a supportive environment for our growing community.

3. TikTok commends PDPC for taking a consultative approach with the industry stakeholders and is committed to working with PDPC to tackle data protection issues relating to minors and develop measures to enhance online safety for Singapore-based users of our services.

4. In the interests of accessibility, TikTok has endeavoured to keep this submission brief but will be pleased to provide more detailed comments where required by PDPC.

5. TikTok wishes to seek confidentiality treatment of this submission. We highlight that parts of this submission refer to the Advisory Guidelines which have not been made publicly available.

II. Comments to Consultation Questions

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?

a. TikTok respectfully suggests that the scope of the proposed Advisory Guidelines should be limited to organisations offering products or services "that are likely to be accessed by children". This would align with the approach taken by children's personal data codes and guidance documents issued by regulators in other jurisdictions, including:

- the United Kingdom's ("**UK**") Age Appropriate Design Code ("**AADC**"), which is stated to apply to online services that are "likely to be accessed by children";[1]
- the California Age Appropriate Design Code which was modeled after the AADC and applies to online services specifically directed at children or which they "are likely to access"[2]; and
- the Irish Data Protection Commission's ("**DPC**") Fundamentals for a Child-Oriented Approach to Data Processing ("**Fundamentals**"), which is stated to apply to services provided by an organisation that is "directed at, intended for or likely to be accessed by children".[3]

Additionally, TikTok is of the view that the scope of the proposed Advisory Guidelines should not go further to also include products or services which are "in fact accessed by children, even if the products or services are not targeted at children". This may create an onerous expectation on organisations to have absolute knowledge of whether children are in fact accessing their products or services, even though the products or services are not designed to be used by, or targeted towards, children. For example, organisations may be required to implement stringent age-verification measures from the outset, which would likely require the collection of personal data beyond what is necessary for the organisation to deliver its products or services to users and contrary to the practice of data minimisation (see also our response to Question 4a. below).

b. TikTok also suggests that the primary obligation of complying with the requirements relating to the protection of children's personal data within the Advisory Guidelines should not apply to organisations that are data intermediaries. This is because organisations (who are data controllers) and data intermediaries play different roles in relation to handling personal data and in interactions with end users, and accordingly the obligations applicable to each such entity should vary accordingly. TikTok notes that the PDPC has also previously explained in its publication *The Distinction between Organisations and Data Intermediaries and Why It Matters*[4] that data intermediaries handle personal data on behalf of data controllers rather than on behalf of the data intermediary itself, and usually do not interact directly with consumers or individuals, hence it is important that consumer-facing requirements are not applied directly to data intermediaries. For example, in the context of children's personal data, it would be difficult for a data intermediary which does not interact with end users to be expected to conduct age-verification measures. Instead, the obligations in respect of protecting children's data should rest on the data controller, who may opt to assign these obligations (where appropriate) to their data intermediaries via contractual methods instead.

---

[1] UK ICO, *Age Appropriate Design: A Code of Practice for Online Services: Services covered by this code* (September 2020).

[2] *California Age Appropriate Design Cod*e Ca. Civ. Code § 1798.99.28

[3] Data Protection Commission (Ireland), *The Fundamentals for a Child-Oriented Approach to Data Processing* (December 2021) 15.

[4] PDPC, *The Distinction between Organisations and Data Intermediaries and Why It Matters*.

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?

TikTok believes that the standard of "reasonableness" in Section 18 of the PDPA should be guided by the principle of taking into consideration the best interests of the child. While we welcome the PDPC's efforts to canvass examples of what the industry and general public would consider to be reasonable purposes for organisations to collect, use or disclose children's personal data, we would caution against converting these examples into a narrow "whitelist" of permitted purposes for the collection, use or disclosure of personal data. As noted by the PDPC in its *Advisory Guidelines on Key Concepts in the PDPA*, the crux of the concept of "reasonableness" is that it is an objective standard which is capable of evolving over time.[5] The principle of the best interests of the child would give organisations a better steer on what is objectively reasonable based on the circumstances, whilst at the same time being flexible enough to accommodate for shifting norms and technological changes.

We would highlight that the principle of the best interests of the child is a concept that already features in other areas of Singapore law. Additionally, the adoption of this principle in the context of the processing of children's personal data would align with the approach taken in other jurisdictions, in which the principle has been adopted in children's personal data codes and guidance documents issued by regulators (these for instance UK's AADC and DPC's Fundamentals). privacy reform proposals in Australia also consider this principle to be a key factor that organisations will need to take into consideration when processing children's personal data[6].

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?

TikTok fully agrees that, in respect of organisations providing services that are directed at or are likely to be accessed by children, communications with children should be conducted in a manner so as to best support the child's understanding of that communication. The understanding of the child is important for them to be able to give informed consent to the collection, use or disclosure of their personal data.

In terms of examples of such communications, this may include the use of simplified, child-appropriate language and perhaps using graphics, audio recordings or video content to communicate with children. Similar requirements have been introduced in the UK AADC[7] and DPC's Fundamentals,[8] which both encourage organisations to use a variety of methods to communicate concepts to children apart from via traditional text/writing, such as using diagrams, cartoons, graphics, video and audio content. In this regard, TikTok makes information regarding privacy and security accessible using the same media format that users are accustomed to viewing on the Platform. TikTokTips, a TikTok run account with more than 5.5 million followers has posted a "You're in Control" video series which provides safety and security tips for all users.

Other helpful ways to communicate with children may include creating a dedicated feature, help centre or site tailored for the use of children. For instance, in addition to its Privacy Policy, TikTok maintains specific youth-facing documentation which provide high-level, simple explanations about what personal information is processed on the platform, and how under-18 users can control how their personal information is handled on the platform. These include TikTok's "Youth Portal", which offers information about both in-app tools and educational content that empower young users to keep their account secure and limit their online footprint

[5] Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the PDPA (Revised 1 October 2021)*, 33.

[6] Attorney General's Department, *Privacy Act Review Report* (February 2023).

[7] UK ICO, *Age Appropriate Design: A Code of Practice for Online Services: Transparency* (September 2020).

[8] Data Protection Commission (Ireland), *The Fundamentals for a Child-Oriented Approach to Data Processing* (December 2021) 29-30.

to the degree they feel comfortable, including a "*Define your public presence*" section that provides a key overview of the privacy and security settings available to youth users. TikTok also maintains a page with information about "Teen Privacy and Safety Settings".

TikTok further understands that providing "just in time", and layered notice to users via in-app messaging can be an effective method of reminding users under the age of 18 of how their personal information will be used. For example, before changing their account from private to public, users are provided with a notice summarizing how that change will alter their account settings. Moreover, before posting a video or photo, the Platform prompts users under the age of 16 to consider who can watch their content. Users in this age group are prompted before posting their first content to the Platform to select whether the video will be accessible to the user only, accepted "friends," or to "followers" generally. "Only me" accessibility is pre-selected by default"

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?

a. We agree with the PDPC's emphasis on data minimisation, including in cases where organisations collect personal data to ascertain a user's age. TikTok considers it important for organisations to have in place a holistic age assurance strategy which starts during registration and continues thereafter. This helps to minimise the amount of personal data collected to ascertain a users' age. For example, we have designed and implemented a series of measures as part of our age assurance strategy aimed at detecting underage users, including, but not limited to, the following:

- TikTok is rated as 12+ or "Parental Guidance Recommended" in App Stores enabling parents to block it from being downloaded.
- When individuals sign up to our services, they are required to enter their date of birth at an age gate. This is neutrally presented, which means that we do not indicate to potential new users at the point of signing up what the minimum age requirement is.
- TikTok has technical measures in place designed to detect the use of keywords in account bios, usernames and handles which may indicate that a user is under 13 (e.g. "I am twelve years old", "primary 6" etc.)
- Our human content moderators are trained to consider whether any of the content they review reveals a potentially underage user.
- We encourage people to report suspected underage accounts. If anyone believes that someone under the age of 13 is using TikTok, they can report this to TikTok using its easy-to-access in-app reporting button located in the user's profile. In addition, users may report a suspected underage user to TikTok via a webform (which is hyperlinked in TikTok's Privacy Policy).
- If a suspected underage account is detected, it is referred to our human Underage Moderation Team. The team will review it to determine whether they believe the account holder is under the age of 13 (or 14 depending on the jurisdiction). If they determine this to be the case, the account will be removed. When a user is banned for being underage, they are notified of this by TikTok and are given three options on how they prefer to verify their age, including taking a selfie with their ID to prove their likeness and taking a selfie holding a piece of paper with their date of birth written on it next to a trusted adult (25+).

We would welcome confirmation from the PDPC that it is not mandatory to collect identity documents or government-issued identifiers to carry out age verification, as this goes against the principle of data minimisation:

- The use of identity documents or official identifiers to verify age raises significant data minimisation concerns. Age verification should not depend on the collection of young

people's identity documents, such as their National Registration identity Card ("**NRIC**") numbers, as this would require the collection of even more personal data than an organisation would otherwise require.

- Furthermore, such judicious collection of NRIC numbers is consistent with the PDPC's *Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers*, which provides that NRIC numbers and other national identification numbers should not be collected, used or disclosed unless it is required under the law (or an exception under the PDPA applies), or where it is necessary to establish or verify the identity of the individual to a high degree of fidelity.

We would also be grateful for confirmation from the PDPC that age verification need not be completed at the account registration stage but can form part of a wider age assurance strategy which starts during registration and continues thereafter (in the interests of balancing risk and the need to avoid the over-extensive collection of personal data). Requiring online services to implement the most stringent age verification measures at the account registration stage would likely necessitate the collection of identity documents or government-issued identifiers and it is unclear how this can be reconciled with the requirements of data minimisation.

b. We welcome the PDPC's efforts to canvas ideas on how the automated collection of geolocation data relating to minors should be regulated. However, we would kindly request further guidance from the PDPC on what it considers to be geolocation data so that we can properly contextualise the application on the proposals regarding the collection of geolocation data.

In considering whether additional protections should apply to the collection of geolocation data, this should depend on how identifiable the individual is from the data in question – for instance, approximate location data that positions someone within a country, region or city (e.g. "Central region, Singapore") alone is unlikely to be able to specifically identify an individual. More importantly, the use of approximate location data can also help protect a user's safety. For example, a service may use approximate location data to understand the risk to a user's account. If a user who has accessed a service from Singapore suddenly switches location to another country, this could suggest that the user's account is under attack, and steps can be taken by the service to secure that user's account. TikTok automatically collects approximate location information of its users based on their SIM card and/or IP address. TikTok may also, with the users permission, collect precise location data. Location data is used by TikTok to maintain and enhance the safety and security of the platform and provide users with location-based services, such as advertising and other personalized content to ensure a better user experience.

Therefore, there should be clarity from the PDPC on what it considers to be within the scope of the proposals regarding the collection of geolocation data. A useful reference point would be the privacy reform proposals in Australia which defines "geolocation tracking data" as personal data which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.[9]

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 would highlight that privacy reforms in other jurisdictions have recommended that DPIAs should be conducted where there is collection, use or disclosure of children's personal data on a large scale.[10] Conducting a DPIA in the context of all data processing activity involving the personal data of children may not always be appropriate and it may result in unnecessary burdens being placed on organisations. There is a risk that requiring a DPIA to be carried out each time children's personal data is processed could cause "DPIA fatigue", where DPIAs

[9] Attorney-General's Department (Australia), *Privacy Act Review Report 2022* (February 2023), 5.
[10] Attorney-General's Department (Australia), *Privacy Act Review Report 2022* (February 2023), 124.

become mere rote evaluation carried out by organisations as a box ticking exercise, instead of serving as a valuable tool designed to identify and mitigate the risk of harm.

In relation to the question on what an organisation should consider when conducting a DPIA, the PDPC's *Guide to Data Protection Impact Assessments* provides some examples of what an organisation should consider when conducting a DPIA, which we would also consider to be applicable in the context of the processing of children's personal data.

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?

TikTok is supportive of the age threshold of 13 years to distinguish when a child can give valid consent on his or her own behalf under the PDPA.

In our view, this would promote certainty for organisations which have already ensured that their business practices are aligned with the position in the PDPC's *Advisory Guidelines on the PDPA for Selected Topics*, which states that as a rule of thumb, a minor who is at least 13 years of age would typically be considered to be able to provide consent under the PDPA on his or her behalf.[11] Furthermore, as mentioned by the PDPC in the *Advisory Guidelines on the PDPA for Selected Topics*, this same age threshold also features in other areas of Singapore law, such as under the Employment Act[12] and the film and video classification ratings system published by the Info-communications Media Development Authority of Singapore.[13] Retaining the same threshold would hence be desirable for organisations for consistency with their business practices in other areas.

Additionally, retaining the 13-year age threshold would also promote standardisation and certainty for regulated entities that operate internationally. This is because this age threshold aligns with the position adopted in several other key jurisdictions, such as the United States (under the Children's Online Privacy Protection Act, where restrictions apply to the collection of personal data of those under 13 years of age), the UK, Spain, Norway and Belgium (each of which adopt the age threshold of 13 years of age in relation to requirements around consent).

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 welcome the Basic and Enhanced Practices listed in the *Guide to Data Protection Practices for ICT systems* as it serves as a useful reference point for measures which organisations handling children's personal data can incorporate to safeguard personal data under their care. However, we would caution against prescribing the Basic and Enhanced Practices for the handling of children's personal data on a best practice basis. This could present itself as a significant challenge for businesses, given that the scope of the Basic and Enhanced Practice

[11] Personal Data Protection Commission, *Advisory Guidelines on the PDPA for Selected Topics (Revised 17 May 2022)*, 57.

[12] As mentioned in page 57 of the Advisory Guidelines on the PDPA for Selected Topics, according to section 68(3) of the Employment Act and Regulation 3 of the Employment (Children and Young Persons) Regulations, a child 13 years of age or older may be employed in light work suited to his capacity in a non-industrial undertaking, and no child who is below the age of 13 years shall be employed in any occupation (with limited exceptions).

[13] The film and video classification ratings system can be accessed at Films | IMDA - Infocomm Media Development Authority.

is rather extensive and may not always be appropriate to the specific circumstances of the data processing.

We strongly believe that personal data protection requirements should be technology-neutral to both cater for the diverse way that personal data is currently handled (e.g. offline and online methods) and for future technologies that have yet to be developed. In our experience, prescriptive data protection standards (even if imposed on a best practice basis) increase compliance costs for organisations and may not always result in tangible benefits for end users. The measures applicable to the handling of children's personal data should be proportionate to the nature of the personal data and the types and purposes of processing..

Therefore, it should ultimately be up to the organisations themselves to decide what combination of data handling measures are most appropriate and proportionate to the processing being carried out, having regard to the spirit of the PDPA and advisory guidelines developed by the PDPC. Organisations are often best placed to understand the risks their service may pose (if any) and how best to safeguard the personal data that is in their possession or under their control.

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?

TikTok is supportive of the PDPC's proposal for an organisation to inform the child's parent or guardian of a notifiable data breach in certain circumstances where feasible. However, we would request that the PDPC specifically recognise that notification to the child's parent or guardian is not required for individuals above the age of 13, as this aligns with the PDPC's view that a person above 13 years of age will have sufficient understanding to be able to provide consent. Individuals above 13 years of age and with such sufficient understanding should also have sufficient grasp of the consequences of a data breach for their privacy.

III. Conclusion

TikTok recognises and supports the understanding that children deserve specific protection in the online sphere due to the increasing amounts of time which children spend online, especially when it comes to the collection, use and disclosure of their personal data. We are very grateful for the opportunity to provide our feedback on the Advisory Guidelines and will be pleased to provide more detailed comments on our submissions, if required by the PDPC.