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

OC QUEEN STREET LLC

5 September 2023

Koh Chia Ling
Managing Director
chialing.koh@ocqueenstreet.com

Giam Zhen Kai
Associate
zhenkai.giam@ocqueenstreet.com

Lim Wei Jie
Associate
weijie.lim@ocqueenstreet.com

A. INTRODUCTION

1. OC Queen Street LLC ("**OCQS**") extends its appreciation and thanks to the Personal Data Protection Commission ("**PDPC**") for the opportunity to comment on the *Public Consultation on the Proposed Advisory Guidelines on the Personal Data Protection Act for Children's Personal Data* (the "**Consultation Paper**").

2. We are a Singapore law practice affiliated with the Osborne Clarke's (collectively, "**OC**") international, technology-focused law practice with offices in the United Kingdom, United States, Europe and China. We provide commercial and regulatory support to digital businesses and fintech companies and are regularly called upon to advise on data protection and cybersecurity matters.

3. OC is ranked as a global Top 10 "elite" law firm for data-related matters and a global Top 5 firm for data litigation by the Global Data Review's GDR 100 2023 rankings. OCQS and its Managing Director, Mr. Chia-Ling Koh, have been recognised as a leading law firm and lawyer respectively in the Legal 500 and Chambers & Partners rankings. Many of our clients have given us positive feedback on our work. Here are some of the testimonials we received:

   "*The firm's data practice forms part of its digital business offering, and is split across the M&A, IP, regulatory, banking, venture capital, private equity, disputes and competition teams. Companies that turn to the firm hail from the fintech, medtech, AI, e-commerce, telecoms, proptech, cybersecurity and e-payments subsectors; the practice also serves traditional companies that are going through digitalisation*." – Global Data Review, 2019

   Chia Ling has been described as being "*well versed in telecoms regulatory advice, as well as a variety of technology issues, including data privacy and contactless payments. Also handles technology transactions*." –Chambers TMT Asia Pacific 2019

4. We have reviewed the Consultation Paper and are pleased to provide our comments below and highlight our concerns for further consideration.

B. OUR COMMENTS ON THE QUESTIONS IN PART II OF THE PROPOSED ADVISORY GUIDELINES

No.	Question	Comments
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. We generally support the extension of the Advisory Guidelines to organisations that "*offer products or services that are likely to be accessed by children, or are in fact accessed by children*". However, we propose that organisations which expressly do not contract with children be excluded from the scope of the Advisory Guidelines. In our view, applying the Advisory Guidelines without the exclusion above would impose a disproportionate compliance cost on all organisations. Organisations would need to conduct assessments to determine whether their products or services *"are in fact accessed by children*", even if these organisations expressly do not contract with children. Organisations would also have to bear the risk of being caught by the Advisory Guidelines if children access their products or services under a false identity / with a false age declaration. Therefore, we believe that a fairer approach would be to exclude organisations which expressly do not contract with children. b. We support the extension of the protection requirements in the Advisory Guidelines to data intermediaries processing children's personal data.
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	Before discussing what we view are reasonable purposes for the collection, use or disclosure of personal data, we would first like to state that the general legal position that contracts with minors

No.	Question	Comments
	circumstances. What are examples of reasonable purposes for organisations to collect, use, or disclose children's personal data?	below the age of 18 have no effect[1] with the exception of the following contracts ("**exceptional contracts**"): - Contracts for necessaries.[2] - Contracts for the benefit of minors such as contracts for service, training or education or analogous arrangements.[3] - Contracts voidable at the instance of the minor such as contracts involving the acquisition of interests in land, the acquisition of or subscription for shares, partnerships and marriage settlements.[4] On its face, the collection, use and disclosure of children's personal data by organisations should therefore be limited to (i) the above exceptional contracts, (ii) contracts executed on behalf of children by their parent or legal guardian or (iii) non-contractual situations (i.e., where the relationship between organisation and child is governed by statute). In view of the above, the collection, use or disclosure of children's personal data for the following non-exhaustive purposes would appear to be reasonable:

[1] Civil Law Act 1909 ("**CLA**"), section 35(1) r/w Women's Charter 1961 ("**WC**"), section 2(1).
[2] Sale of Goods Act 1979, section 3(2). A minor is bound to pay a reasonable price for such necessaries.
[3] *Clements v London and North Western Railway Co* [1894] 2 QB 482; see also Andrew Phang, *The Law of Contract in Singapore* (Academy Publishing, 2012) at [09.007] to [09.010] ("**Phang**").
[4] Phang, [09.011].

No.	Question	Comments
		a. Administration or provision of educational or training programmes or courses. b. Provision of medical treatment. c. Provision of counselling or therapy services. d. Marketing in connection with the exceptional contracts described above, to the extent a Data Protection Impact Assessment (DPIA) is carried out.[5] In contrast, the collection, use or disclosure of children's personal data for the following non-exhaustive purposes would, in our view, not be reasonable: a. The entry into and performance of a contract with a child that is invalid.[6] b. The display of content that is expressly prohibited by law (e.g., "*egregious content*" defined in section 45D(1) of the Broadcasting Act 1994 or content that discloses an offence under the First Schedule of the (to-be-commenced) Online Criminal Harms Act).

[5] In the context of the UK General Data Protection Regulations (GDPR), the UK Information Commissioner's Office (ICO) requires that a DPIA be conducted when organisations intend to profile children or target marketing or online services at them, since marketing is deemed a "high-risk" activity. See https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/ for more details.

[6] For example, contracts for the employment of children and young persons as permitted under Part 8 of the Employment Act 1968 and the exceptional contracts described in our answer to question 1.

No.	Question	Comments
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? -	In our view, when communicating with children between 13 to 17 years of age, organisations should focus on using plain English. We believe children in this age band would have a basic level of English competency since this age band covers Secondary 1 to JC 1 (and equivalent) students who would be studying English as a first language. When communicating with children below the age of 13, in line with the UK Information Commissioner's Office ("**ICO**") guidance,[7] organisations should employ the following: a. (ELI5 Language) Plain and simple language commensurate to the expected competency of children of that age. Technical terminology should be minimised, and if used, should be accompanied with an understandable explanation. b. Cartoons, graphics or videos explaining the different scenarios under which personal data will be collected, used or disclosed. c. Diagrams or flowcharts detailing personal data flows. d. Layered and just-in-time notices ensuring that the most pertinent information is presented at appropriate times.

[7] See here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/how-does-the-right-to-be-informed-apply-to-children/#a2.

No.	Question	Comments
		Organisations should also provide information about data subject rights under the PDPA and how to withdraw consent and complain about personal data handling.
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 assume that organisations are ascertaining their users' age for the purposes of determining whether their users are children whose personal data should be processed in accordance with the Advisory Guidelines. We also assume that these organisations are not organisations who expressly do not contract with children. To minimise collection, use and disclosure, organisations should be able to rely on a self-declaration of the child's age to satisfy themselves of their users' age. If necessary, organisations may ask for other corroborating information such as the child's school or telephone number (or the telephone number of their parent or legal guardian) for verification purposes. Organisations should not collect personal data such as a copy of the child's NRIC or photo unless the collection of such data is in the best interests of the child. b. Geolocation data should only be collected where necessary to fulfil the purposes for which they were collected, assuming those purposes fulfil the reasonableness requirement in section 18 of the PDPA. Geolocation should be switched off by default and only enabled by the user.
5	What are examples of situations where an organisation should conduct a Data Protection Impact Assessment (DPIA) before	It is generally acknowledged that children may lack sufficient awareness of the risks and consequences of the processing of their personal data, and the processing of their personal data

No.	Question	Comments
	releasing products or services likely to be accessed by children? What should an organisation consider when conducting such DPIA?	may require specific protection.[8] In our view, it is good practice for organisations to conduct a DPIA if there is a risk that the processing of children's personal data may result in a high potential adverse effect / significant harm to the affected children in the event of a data breach. Such situations include: a. In line with the UK ICO's guidance,[9] when personal data is collected, used or disclosed for marketing purposes, especially when there is profiling or targeting involved. b. When sensitive personal data is collected, used or disclosed (i.e., NRIC numbers, health or financial data, or any of the categories of personal data listed in the Schedule to the Personal Data Protection (Notification of Data Breaches) Regulations 2021). In our view, in line with the PDPC's Guide to Data Protection Impact Assessments,[10] it is good practice for organisations to consider the following when conducting a DPIA in connection with the collection, use or disclosure of children's personal data:

[8] See, for instance, Recital 38 of the UK GDPR: "*Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*."
[9] See here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-if-we-want-to-target-children-with-marketing/.
[10] See here: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.pdf.

No.	Question	Comments
		a. The likelihood and severity of the potential adverse effects / harms to the affected children. b. Whether any measures can be taken to mitigate or eliminate the potential adverse effects / harms to the affected children. c. Whether there are any residual potential adverse effects / harms to the affected children after the measures in (b) have been adopted. d. What remediation measures are in place in the event any of the risks identified in the DPIA materialise. e. The individuals who should be notified in the event a notifiable data breach occurs. A DPIA is not necessary if an organisation expressly does not sell goods or services to children.
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 welcome the PDPC's adoption of the "*practical view*" that children between the ages of 13 to 17 will have sufficient understanding to consent to the collection, use or disclosure of their personal data. This is a pro-business approach that will be welcomed by organisations. However, this "*practical view*" may be subject to limitations outlined below. It is not clear how an organisation may validly obtain consent from a child below 18 via contractual means if the general contract law position is that contracts with children below 18

No.	Question	Comments
		have no effect, save for the exceptional contracts described in our answer to question 2 above.[11] Section 4(6) of the PDPA provides that the PDPA provisions will not affect any "*limitation imposed, by or under the law*", and the "*provisions of other written law prevail*" to the extent that the PDPA provisions are inconsistent with the provisions of such other written law (that is, statutes and subsidiary legislation in Singapore). In other words, the provisions of the PDPA are presently subject to the limitations imposed by common law, statute and subsidiary legislation on the validity of contracts with minors (eg. section 35(1) of the Civil Law Act 1909 ("**CLA**") r/w section 2(1) of the Women's Charter 1961 ("**WC**")). If the PDPC's intention is to allow minors below 18 to consent via contractual means to the collection, use and disclosure of their personal data, then legislative amendments may have to be made to remove the limitations on the PDPA in section 4(6) of the PDPA. It appears that to seek valid consent in cases where the contract is of no effect, an organisation must seek non-contractual consent. However, it remains to be determined by the courts whether as a matter of policy, an organisation may obtain valid non-contractual consent for the purposes of, say, entering a contract which has no effect. The legal position and proposed workaround we have

[11] See footnote 6.

No.	Question	Comments
		highlighted above are based on a cursory review of the law and should be explored in greater detail.
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?	No comment.
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?	In our view, where consent is obtained via a contract with a child below 18 that is not an exceptional contract described in our answer to question 2 above, an organisation should inform the child's parent or legal guardian in the event a notifiable data breach occurs. This is because of the general contract law position that contracts with children below 18 are of no effect and any consent given pursuant to such contracts would, naturally, also be invalid under the law as it currently stands. Admittedly, personal data should not have been collected in the first place. In the absence of the above contractual limitations, then it would be prudent for organisations to notify the child's parent or legal guardian in the event a notifiable data breach occurs if doing so is in the welfare and best interests of the child.[12] For instance, it

[12] The best interests of the child is recognised as a guiding principle in section 4 of the Children and Young Persons Act 1993 ("**CYPA**") and Article 3 of the United Nations Convention on the Rights of the Child ("**UNCRC**") (acceded by Singapore on 2 October 1995).

No.	Question	Comments
		may be in the welfare and best interests of the child to notify the child's parent or legal guardian if there is a risk that the data breach: a. Will result in the abduction, abuse, or commercial or sexual exploitation of the child. b. Will adversely affect the health and wellbeing of the child. c. Will adversely affect the child's identity or reputation. In determining where the child's best interests and welfare lie, it may be prudent for organisations to refer to the UN Convention on the Rights of the Child ("**UNCRC**") (acceded by Singapore on 2 October 1995) which sets out the civil, political, economic, social, health and cultural rights of children.

(the rest of this page is intentionally left blank)

C. CONCLUSION

1. We welcome the implementation of the Advisory Guidelines and hope that the PDPC will take into account our views highlighted above, namely:

   (a) The Advisory Guidelines should not apply to organisations that expressly do not contract with children.

   (b) Based on a cursory review of the law, contracts with minors below the age of 18 generally have no effect unless such contracts are exceptional contracts (discussed in our response to question 2 above). In the circumstances:

      (i) While we welcome the PDPC's "*practical view"* that children between the ages of 13 to 17 may consent to the collection, use and disclosure of personal data, legislative amendments may have to be made if the PDPC's intention is to allow minors below 18 to consent via contractual means. This is because the PDPA is subject to limitations imposed under the law and the provisions of other written law prevail over the PDPA.

      (ii) It appears that to seek valid consent in cases where the contract is of no effect, an organisation must seek non-contractual consent. However, it remains to be determined by the courts whether as a matter of policy, an organisation may obtain valid non-contractual consent for the purposes of entering a contract which has no effect.

   N.B. The legal position and proposed workaround we have highlighted above are based on a cursory review of the law and should be explored in greater detail.

   (c) One of the reasonable purposes for which the collection, use and disclosure of personal data should be permitted is marketing in connection with exceptional contracts. However, a DPIA should be conducted prior to such activities in certain circumstances given that marketing is an activity that may result in a potential adverse effect / significant harm to the child.

   (d) Organisations communicating with children between the ages of 13 to 17 on privacy matters should focus on using plain English. Organisations communicating with children below 13 on privacy matters should use ELI5 language, cartoons, diagrams or flowcharts as appropriate. Organisations should also provide information about data subject rights under the PDPA and how to withdraw consent and complain about personal data handling.

   (e) Organisations verifying their users' age should be able to rely on a self-declaration of the age to satisfy themselves of their users' age. If necessary, organisations may ask for other corroborating information such as the child's school or telephone number (or the telephone number of their parent or legal guardian) for verification purposes. Organisations should not collect personal data such as a copy of the child's NRIC or photo unless the collection of such data is in the best interests of the child.

   (f) When a notifiable data breach occurs, organisations should inform the child's parent or legal

guardian if consent is obtained via a contract with a child below 18 that is not an exceptional contract. Admittedly, personal data should not have been collected in the first place.

In other cases, then it would be prudent for organisations to notify the child's parent or legal guardian in the event a notifiable data breach occurs if doing so is in the welfare and best interests of the child. Organisations may consider referring to the UNCRC to determine what is in the welfare and best interests of the child.

OC QUEEN STREET LLC
5 September 2023