PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

RESPONSE TO FEEDBACK ON PUBLIC CONSULTATION ON PROPOSED ADVISORY GUIDELINES ON THE PDPA FOR CHILDREN'S PERSONAL DATA IN THE DIGITAL ENVIRONMENT

Issued 28 March 2024

Supported by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In support of:

SG:DIGITAL

TABLE OF CONTENTS

PART I: INTRODUCTION

1 Background

1.1 The Personal Data Protection Commission ("PDPC") launched a public consultation on 19 July 2023 on the proposed Advisory Guidelines on the Personal Data Protection Act for Children's Personal Data in the Digital Environment ("Advisory Guidelines")[1].

1.2 The proposed Advisory Guidelines aim to provide guidance and best practices to industry on:

a) How valid consent may be obtained from children, defined as an individual who is below 18 years of age (consistent with the Code of Practice for Online Safety[2] under the amended Broadcasting Act);

b) According to higher protection standards to children's personal data as sensitive data; and

c) How children's data / profiles may be used.

1.3 The consultation closed on 31 August 2023 with 15 responses from organisations representing various sectors (e.g. finance, tech, education) and an individual. For the full list of respondents and their submissions, refer to the PDPC's website[3]. The PDPC thanks all respondents for the comments submitted to the public consultation.

1.4 This note summarises the key matters raised by respondents and provides the PDPC's responses.

[1] The Advisory Guidelines should be read in conjunction with Chapter 8 of the Advisory Guidelines on the PDPA for Selected Topics (Data Activities Relating to Minors).
[2] The Code of Practice for Online Safety was issued by IMDA on 17 Jul 2023 and took effect from 18 Jul 2023.
[3] Available at <https://www.pdpc.gov.sg/guidelines-and-consultation/2023/07/public-consultation-on-the-proposed-advisory-guidelines-on-the-pdpa-for-childrens-personal-data>.

PART II: OVERVIEW OF ISSUES

2 Scope of the Advisory Guidelines

2.1 The public consultation sought feedback on the PDPC's proposed scope of the Advisory Guidelines. The proposed scope:

a) Covers organisations that offer products or services that are (i) likely to be accessed by children, or (ii) are in fact accessed by children, even if the products or services are not targeted at children; and

b) Considers that the requirements relating to the protection of children's personal data within the Advisory Guidelines will apply to organisations that are data intermediaries ("DIs").

Summary of feedback

2.2 Responses supported the intent of the Advisory Guidelines but sought clarity on its scope. There were calls for alignment to UK ICO's Age-Appropriate Design Code ("Children's Code"). Specifically, that the Advisory Guidelines should mirror the Children's Code's scope of being "likely to be accessed by children"[4]. There was also feedback that organisations should not be able to circumvent the PDPC's guidelines by merely stating that their content, products, or services, are not intended for minors.

2.3 Concerning (b), responses agree that the relevant requirements on DIs should continue to apply. In addition, DIs should not be subject to "consumer-facing requirements", such as ensuring that valid consent were obtained. Clarifications were also sought on the definition of a DI under the PDPA.

PDPC's response

2.4 The PDPC recognises that the Children's Code is among the leading standards on online safety and data protection for children's personal data. Together with the OECD's Recommendation on Children in the Digital Environment[5], such standards seek to balance between protecting children and promoting the benefits that the digital environment can provide.

[4] The UK Children's code applies to "information society services ("ISS") likely to be accessed by children". This is not limited to services that are designed for and aimed specifically at children, but also services that children are using in reality, e.g. where there is evidence that a significant number of children are in fact accessing the service. For more information - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/

[5] For more information on the recommendations by OECD (Organisation for Economic Co-operation and Development) - https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389?_ga=2.48796774.1171367707.1703058247-404839653.1703058247

2.5 In view of the feedback, the PDPC clarifies that the Advisory Guidelines is aimed at organisations whose online products or services are likely to be accessed by children. Organisations should not circumvent the Guidelines by merely stating that their products or services are not intended for children.

2.6 The following are examples of products and services which fall under this scope:

a) Social media services, as defined in section 45T of the Broadcasting Act 1994;

b) Technology aided learning ("EdTech");

c) Online games; and

d) Smart toys and devices.

2.7 Under the PDPA, a DI is defined as an entity that processes personal data "on behalf of another organisation." A DI is subject to the Data Protection Provisions relating to protection of personal data ("Protection Obligation"), retention of personal data ("Retention Limitation Obligation") and notifying an organisation of data breaches ("Data Breach Notification Obligation") when it is processing personal data on behalf of that organisation and for that organisation's purposes.

2.8 Organisations engaging a DI should conduct due diligence to ensure that the DI is able to meet its data processing requirements and provide the protection and care that is commensurate with the volume and sensitivity of the personal data that the DI is to process. For more information on managing DIs, refer to the PDPC's Guide to Managing Data Intermediaries.

3 Reasonable purposes for children's personal data

3.1 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. The public consultation sought examples of reasonable purposes for organisations to collect, use or disclose a child's personal data.

Summary of feedback

3.2 A few responses cautioned against prescribing a list of reasonable purposes and asked for a principles-based approach. Examples of reasonable purposes provided include the registration for a book club and the opening of a bank savings account.

PDPC's response

3.3 The PDPC will adopt a principles-based approach and provide guidance in the Advisory Guidelines on what the PDPC considers to be reasonable when collecting,

using, or disclosing children's personal data.

4 Communication with children

4.1 When communicating with children, organisations should use language that is readily understandable by children. The public consultation asked for views and examples of such communication with children.

Summary of feedback

4.2 Responses agreed that language used in communicating with children should be readily understandable by a child. There were clarifications on the definition of "readily understandable". Organisations suggested that they should have the flexibility to assess and implement the appropriate communications methods that are relevant to their specific target audience.

PDPC's response

4.3 The PDPC recognises that children are unique individuals with varying developmental abilities. While there is no one size-fits-all approach when communicating with individuals of this age bracket, the PDPC will provide guidance in the Advisory Guidelines on what organisations should consider and implement when communicating with children.

5 Data minimisation

5.1 The PDPC asked how organisations should minimise the collection, use, and disclosure of children's personal data:

a) when ascertaining their users' age; and

b) when collecting geolocation data.

Summary of feedback

5.2 For (a), responses cautioned against the prescription of specific methods to ascertain an individual's age. Organisations should be allowed the latitude to assess and employ the relevant measures based on their business needs. Questions raised include (i) whether age verification should be limited to the account registration stage, and (ii) whether the PDPC considers it mandatory to collect national identification documents.

5.3 Regarding (b), a few responses noted that certain products and services would require geolocation data for them to function optimally. Other responses stated that geolocation data should be disabled by default and collected only with consent.

PDPC's response

5.4 The PDPC supports the use of age assurance methods for the purpose of conforming to the Advisory Guidelines, including age verification or estimation methods to ascertain if the user is a child or adult. Effective age assurance methods help organisations to better estimate a user's age and implement relevant safeguards when the user is a child.

5.5 Geolocation data is considered personal data when an individual can be uniquely identified when the geolocation data is combined with other identifiers. To balance between the risk of misuse and the need for geolocation data (e.g. where a product or service requires the data to function), organisations collecting geolocation data should adopt a data minimisation approach to collect the least amount of data that is necessary for the purpose. More guidance will be provided in the Advisory Guidelines.

6 Data Protection Impact Assessment ("DPIA")

6.1 The PDPC asked for 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. The PDPC also asked for the considerations that organisations should note when conducting a DPIA.

Summary of feedback

6.2 Some responses called for DPIAs to be conducted for all products and services targeted at children. There were also concerns that mandating DPIAs will impose a high regulatory burden on organisations.

PDPC's response

6.3 The PDPC notes that DPIAs are beneficial for organisations and consumers. Conducting DPIAs can help organisations to identify potential data protection risks, enabling them to take proactive mitigatory measures. Through the DPIA process, organisations demonstrate their commitment to accountability in handling personal data, which can lead to increased trust from consumers.

6.4 Organisations are advised to conduct DPIAs when necessary to develop and implement policies and practices to meet the Accountability Obligation under the PDPA. In addition, organisations are encouraged to conduct a DPIA before releasing products or services that are likely to be accessed by children, so that they can identify and address personal data protection risks. The PDPC will provide further guidance in the Advisory Guidelines on questions which organisations can consider when conducting a DPIA.

7 Consent by and notification to children

7.1 The PDPC noted in the public consultation that the age threshold of 13 years appears to be a significant one in relation to the protection of minors[6], and is considering the view that a child 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 to withdraw such consent. Accordingly, the PDPC sought for views on when a child can give valid consent under the PDPA.

Summary of feedback

7.2 Many responses agreed with the age threshold of 13 years old, noting that the age is similar to prevailing laws in other jurisdictions (e.g. the US, Canada, the UK, Spain). A few responses sought for a higher age threshold (e.g. 15, 16 and 18), but there was no consensus on the exact age. Clarifications were sought on (i) the interaction between the PDPA and other local laws, and (ii) whether the consent provided by a child is still valid when the child reaches 18 years old.

PDPC's response

7.3 The PDPC considers that a child between 13 and 17 may give valid consent, when the policies on the collection, use and disclosure of the child's personal data, as well as the withdrawal of consent, are readily understandable by them. However, where an organisation has reason to believe that a child does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from the child's parent or guardian. Further guidance on this area will be provided in the Advisory Guidelines.

7.4 On the PDPA's interaction with other laws, organisations are reminded that if there is any inconsistency between another written law and the data protection provisions in the PDPA, the other written law will prevail to the extent of the inconsistency.

8 Protection measures

8.1 As children's personal data is of a more sensitive nature, organisations are required to take extra precautions and ensure higher standards of protection under the PDPA regarding such data. The public consultation asked for views on the practices listed

[6]For example, under the Employment Act, 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 a limited exception) – please see section 68(3) of the Employment Act and Regulation 3 of the Employment (Children and Young Persons) Regulations. Similarly, some film and video classification ratings set out age thresholds for audiences for such content, including Parental Guidance 13 ("PG13"). PG13 is an advisory rating that means "suitable for persons aged 13 and above but parental guidance is advised for children below 13". More details of the film and video classification system are available at: https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/films..

in the PDPC's Guide to Data Protection Practices for ICT systems and if there are additional measures organisations should undertake to protect children's data.

Summary of feedback

8.2 While responses agree on the need for higher standard of protection for children's data, there were cautions against mandating specific measures as not all measures are appropriate or relevant.

PDPC's response

8.3 Given the sensitive nature of children's personal data, organisations should implement, where appropriate, the applicable Basic and Enhanced Practices listed in the PDPC's Guide to Data Protection Practices for ICT Systems to address potential risks and harms to children. To meet the objective of protecting children's personal data under their care, organisations may also implement additional or alternative measures. Further guidance will be provided in the Advisory Guidelines.

9 Data breach notification to children's parents or guardians

9.1 The public consultation sought for views on the circumstances in which it would be prudent for an organisation to inform the child's parent or guardian of a data breach. This would allow the parent or guardian to take steps to mitigate the harm to the child from a data breach.

Summary of feedback

9.2 Feedback agreed on the need to notify children (and parents, where applicable) when a breach is notifiable under the PDPA. Clarifications were sought on how to notify parents / guardians if the organisation does not have their contact details.

PDPC's response

9.3 In the case of a data breach resulting in significant harm to individuals who are children, the organisation's obligation to inform the affected data subject remains, even though the data subject is a child.

9.4 Organisations are encouraged to inform the child's parent / guardian of the data breach where feasible (when the organisation has the contact details of the parent / guardian), since this allows the child's parent or guardian to take steps to mitigate the harm of the data breach. Further guidance will be provided in the Advisory Guidelines.

PART III: CONCLUSION

10.1 The PDPC will continually assess the need to provide further guidance through Advisory Guidelines, technical guides, or other resources to assist organisations in meeting their obligations under the PDPA. Organisations should visit www.pdpc.gov.sg for more information.

10.2 Once again, the PDPC thanks all respondents for their comments submitted to this public consultation.

END OF DOCUMENT