PERSONAL DATA PROTECTION COMMISSION SINGAPORE

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 Introduction

1.1 In today's highly connected world, children start using the Internet at a young age and may not fully grasp the risks, or understand the consequences, of sharing their personal data. While parents play an important role in guiding and protecting children in this digital environment, organisations can also play a significant role in ensuring that the products or services that they offer adopt a data protection by design[1] approach. This would ensure that children's personal data are protected, and that they can safely benefit from participation in the online space.

1.2 These Advisory Guidelines clarify how the data protection provisions in the Personal Data Protection Act 2012 ("PDPA") apply to children's personal data in the digital environment. However, these Guidelines are not exhaustive, and not every section may be applicable to each organisation.

1.3 The Guidelines should be read in conjunction with Chapter 8 of the PDPC's Advisory Guidelines on the PDPA for Selected Topics (Data Activities Relating to Minors) as it covers the application of the data protection obligations on general activities for minors (i.e. individuals who are less than 21 years of age). Organisations should continue to comply with all the relevant data protection obligations under the PDPA, even if not covered in the Guidelines.

1.4 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.

PART II: APPLICATION

2 Scope of application

2.1 The Guidelines apply to organisations whose online products or services are likely to be accessed by children[2]. The following are examples of online products or services which fall under the scope of the Guidelines:

[1] Data Protection by Design ("DPbD") is an approach where data protection measures are considered and built into products or services that involve the processing of personal data as they are being developed. For more information on applying the DPbD approach, refer to the PDPC's Guide to on Data Protection Practices for ICT Systems.

[2] To be clear, the scope is not limited to products and services that are designed for and aimed specifically at children, but also covers products and services that children access in reality.

a. Social media services, as defined in section 45T of the Broadcasting Act 1994[3];

b. Technology aided learning ("EdTech");

c. Online games; and

d. Smart toys and devices.

2.2 For the avoidance of doubt, chapters 6 and 7 of these Guidelines also apply to organisations that are data intermediaries.

2.3 For the purposes of these Guidelines:

a. "age assurance" refers to methods for ascertaining a person's age and includes self-declaration, age estimation, and age verification;

b. "age estimation" refers to the estimation of an individual's age or age range;

c. "age verification" refers to the verification of an individual's age or confirmation that an individual is above a certain age (e.g. below 18 years of age);

d. "child" or "children" refers to an individual or individuals who is or are below 18 years of age; and

e. "geolocation" refers to the ability to determine the physical location of a device.

3 Notification

Communication with children

3.1 The Commission recognises that children are unique individuals with varying developmental abilities. While there is no one-size-fits-all approach when communicating with individuals within this age bracket, organisations should

[3] "Social media service" means an electronic service that satisfies all the following characteristics:

(*a*) the sole or primary purpose of the service is to enable online interaction or linking between 2 or more end-users (including enabling end-users to share content for social purposes);

(*b*) the service allows end-users to communicate content on the service;

(*c*) any other characteristics that are prescribed by Part 10A regulations;

consider the nature of their content and adopt age-appropriate language and media (e.g. infographics, video clips).

3.2 When communicating with children, organisations must use language that is readily understandable by children so that children may understand the consequences of providing and withdrawing consent. This means that the notification of purpose and consent clauses, data protection policies, and terms and conditions, must be in language that is readily understandable by children[4].

Example: Ensuring language is readily understandable

An organisation's account-based online game is accessible by individuals of all ages, including children. When communicating with children, the organisation should use plain and simple language, and avoid deceptive language or design. The organisation can also consider using visual and audio aids to support the child's understanding.

One way that the organisation ensures that the language is readily understandable is by conducting a trial run of their product or service with children of varying ages and adjusting the language accordingly to ensure that it is readily understandable.

4 Consent for collection, use, or disclosure of personal data

Giving valid consent under the PDPA

4.1 Section 13 of the PDPA provides that organisations are allowed to collect, use, or disclose an individual's personal data if the individual gives his or her consent for the collection, use, or disclosure of it.

4.2 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. This includes ensuring that the child understand the consequences of providing and withdrawing consent. 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.

4.3 There may be instances where an organisation will consider a higher age of consent more appropriate in its business context. For example, an organisation in an education setting may assess that it is more prudent to obtain consent from a parent

[4] This includes the relevant information organisations are required to inform individuals as part of fulfilling Section 20 ("Notification Obligation") of the PDPA. For more information on the Notification Obligation, see Chapter 14 of the Advisory Guidelines on Key Concepts in the Personal Data Protection Act.

of a 13-year-old rather than to directly seek the consent of a 13-year-old. In such cases, the organisation should proceed to do so.

4.4 Organisations should also ensure that children are able to withdraw consent for their personal data as easily as providing consent for their personal data.

4.5 Where the child is below 13 years of age, the organisation must obtain consent from the child's parent or guardian[5]. The parent or guardian should be notified of the purpose(s) for which the child's personal data will be collected, used, and disclosed.

4.6 The PDPC considers consent that was previously obtained from an individual (or parent / legal guardian) when he / she was a child to remain valid when the individual reaches 18 years of age.

5 Reasonable purposes for the collection, use, and disclosure of children's personal data

5.1 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 in the circumstances. For example, a purpose that is in violation of the law or which would be harmful to the individual concerned is unlikely to be considered appropriate by a reasonable person.

5.2 The PDPC will continue to adopt a principles-based approach to consider what is reasonable when collecting, using, or disclosing a child's personal data. Given the potential risks and harms to children in the digital environment, examples of what is reasonable include, but is not limited to:

a. collecting and using a child's personal data or profile for age assurance to ensure that only age-appropriate content is accessible;

b. collecting and using a child's personal data or profile to protect the child from harmful and inappropriate content; and

c. using the behavioural data of a child, such as the use of high-risk search terms including terms relating to self-harm or suicide, to direct the child to relevant safety information.

[5] Section 14(4) of the PDPA provides that consent given or deemed to have been given by an individual for the collection, use, or disclosure of the individual's personal data, includes consent given or deemed to have been given by any person validly acting on behalf of that individual for the collection, use, or disclosure of the personal data.

5.3 The PDPC will consider as unreasonable, the use of a child's personal data or profile to target harmful or inappropriate content (as defined in the Code of Practice for Online Safety[6]) at the child.

5.4 In addition, organisations should adopt data minimisation[7] policies to limit the collection and sharing of children's personal data. For instance, the account information of children must not be made public and searchable, by default.

Ascertainment of age

5.5 The PDPC supports organisations' use of age assurance methods for the purpose of conforming to these Guidelines, including age verification or estimation methods to ascertain the user's age, so that organisations can implement relevant safeguards when the user is a child. While doing so, organisations should practice data minimisation and collect the minimum amount of personal data necessary for those age ascertainment purposes.

> **Example: Prompting users to take breaks during gameplay**
>
> An organisation's online game is accessible by children and does not require a user to sign up for an account before the user can play the game. The organisation wishes to prompt users to take breaks from extended gameplay. The organisation can use age estimation methods to estimate the age or age range of the user, so that if the user is likely to be a child, the game can remind the user to take a break.

5.6 Organisations performing age assurance do not have to limit themselves to the account registration stage and may do so at appropriate juncture(s). In addition, unless required under applicable laws, organisations are not required to collect national identity documents for age assurance purposes.

5.7 The PDPC is aware that some age assurance methods involve the collection and analysis of the behavioural and telemetric data of users to build profiles[8] that are used to ascertain the age or age range of individual users. Organisations should take note that once they have collected data about a user to such an extent that the user

[6] Issued under the Broadcasting Act 1994.

[7] For more information on data minimisation, see the PDPC's Guide to Data Protection Practices for ICT Systems.

[8] A profile of an individual is a representation of him or her. Online profiling refers to the collection of information about an individual, for example his or her personal data or online behaviour, to create a profile of the individual's interests and habits. Profiles of individuals, including children, are commonly used to suggest or serve content (e.g., advertisements) to them.

can be identified from that data, or from that data and other information to which the organisation has or is likely to have access, then the user profile will be personal data.

Example: Whether the data collected is considered personal data

An organisation offering social media services does not require a user to sign up for an account before the user can access social media content. The organisation can ask the user to declare his or her age so that if the user is a child, the organisation can provide the user with age-appropriate content and restrict the user from accessing harmful or inappropriate content, including in the form of advertisements.

As it would not be possible to identify who the user is based solely on the age declared by the user, the age that was declared by the user is not considered personal data.

However, if browsing history or other behavioural data is collected and associated with the unique identifier of a user such that an individual can be identified from that data, then the data will be considered personal data.

Geolocation data

5.8 Geolocation data refers to data taken from a device which could be used to identify the geographical location of that device. Examples of such data include global navigational satellite system ("GNSS"[9]) data and data from Wi-Fi access points.

5.9 The PDPC considers geolocation data to be personal data to the extent that an individual can be uniquely identified when the geolocation data is combined with other identifiers.

5.10 As the ability to determine or monitor the precise location of a child poses the risk of misuse that may compromise the child's safety, organisations should adopt a data minimisation approach and implement relevant safeguards considering how the product / service would be used by children.

5.11 One safeguard is disabling the geolocation function by default so that precise location data is not automatically collected when a product or service is first used. Other safeguards include collecting users' approximate location rather than precise location. For other good practices, refer to the PDPC's Guide to Data Protection Practices for ICT Systems.

[9] GNSS is the general term used for satellite systems that provide positioning / navigation services. For example, the global positioning system ("GPS") and BeiDou.

Example: Default settings for geolocation data

A child wants to install a photo filter app for children that allow users to take and edit photos. Although the app has a function to tag the precise location of where a photo was taken, this geolocation function should be disabled by default so that precise location data is not automatically collected.

The app should use readily understandable language to notify users and obtain consent prior to any collection, use or disclosure of geolocation data. The app should also consider the granularity of the location data needed and not collect more than necessary. In addition, a prominent symbol could be used to indicate when the geolocation function is enabled or disabled.

6 Protection of children's personal data

6.1 The personal data of children is generally considered to be sensitive personal data and must be accorded a higher standard of protection under the PDPA[10].

6.2 Any organisation that handles children's personal data should implement, where appropriate, the Basic and Enhanced Practices listed in the PDPC's Guide to Data Protection Practices for ICT Systems[11], to address potential risks and harms to children in the digital environment. However, this list does not preclude organisations from implementing additional or alternative measures to fulfil their obligation to protect the personal data in their possession or under their control. Some examples include:

<u>Basic Practices</u>

a. Developing and implementing Infocomm technology ("ICT") security policies for data protection, including policies on account and access control, backup and retention, and passwords.

b. Assessing and mitigating the security risks involved in outsourcing or engaging external parties for ICT services.

[10] See also the PDPC's decision in *Singapore Taekwondo Federation* [2018] SGPDPC 17 at [21]-[27]. The PDPC considered the treatment of minors' personal data in other jurisdictions and concluded that, "[a]gainst this backdrop, minors' personal data would typically be of a more sensitive nature…".

[11] See the PDPC's Guide to on Data Protection Practices for ICT Systems for the most updated lists of measures.

Enhanced Practices

c. Using a one-time password ("OTP") or 2-Factor Authentication ("2FA") / Multi-Factor Authentication ("MFA") for admin access to personal data and logging all access.

d. Conducting network penetration testing prior to the commissioning of any new ICT system to detect and resolve any vulnerabilities before the system goes "live".

7 Data breach notification

7.1 Part 6A of the PDPA sets out the requirements for organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or the PDPC where it is assessed to be notifiable[12].

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

7.3 If an organisation proactively informs the child's parent or guardian of the data breach (if the organisation has the contact details of the parent / guardian), the child's parent or guardian would be able to take steps to mitigate the harm of the data breach.

7.4 Where the organisation does not have the contact details of the child's parent or guardian, the organisation should ensure that the data breach notification to the child is in a language that is readily understandable by the child so that the child may understand the consequences of the data breach. The organisation should also consider advising the child to inform his / her parent or guardian about the data breach.

[12] Organisations should refer to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 on the list of personal data and classes of personal data, of which a breach will be deemed to result in significant harm to an individual, and hence notifiable.

Example: Unauthorised access of students' records

The database administrator of an edtech company discovers an unauthorised access to its student records. The edtech company immediately assesses the data breach and determines that the data breach involves records of students' name and email address. The records of approximately 20 children are affected.

As the data breach only involves students' name and email address, the data breach is deemed to be unlikely to result in significant harm to an individual and the organisation need not notify the affected students of the data breach.

While the edtech company is not required to notify the affected individuals, the edtech company chooses to demonstrate accountability by notifying the affected children's parent (or legal guardian) of the data breach since the relevant contact details were collected during the registration process.

If the edtech company has only the contact details of the child, the edtech company could advise the child, in language that is readily understandable by the child, to notify his / her parent (or guardian).

Notifying allows the child's parent or guardian to take steps to mitigate the harm of the data breach, such as by monitoring the emails sent to their child's account for suspicious content.

8 Accountability

Data Protection Impact Assessments ("DPIA")

8.1 To meet the Accountability Obligation under the PDPA, organisations are advised to conduct DPIAs to help them develop and implement appropriate policies and practices. In addition, organisations are encouraged to conduct a DPIA before releasing products or services that are likely to be accessed by children, to identify and address personal data protection risks[13].

8.2 For sample questions to consider when conducting a DPIA, refer to Annex A.

END OF DOCUMENT

[13] For more information on DPIAs, see the PDPC's Guide to Data Protection Impact Assessments.

Annex A: Sample questions to consider when conducting a Data Protection Impact Assessment ("DPIA")

S/N	Question
General	
1.	Have you familiarised yourself with the guidance provided in the Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment?
Nature of the product or service	
2.	Is the product or service likely to be accessed by children? If so, what is the age or age range of these children?
3.	How will you ascertain the age or age range of a user of the product or service?
Define the context / purpose of collection, use, or disclosure	
4.	Will you be collecting, using, or disclosing a child's personal data? If so: • List the types of personal data that will be collected, used, or disclosed for this purpose. • What is the purpose of collecting, using, or disclosing the child's personal data? • Describe how the personal data will be collected, used, or disclosed.
Consent	
5.	If you are obtaining consent from a child between 13 and 17 years of age for the collection, use, or disclosure of personal data, are your notification of purpose and consent clauses, data protection policies, and terms and conditions, in a language that is readily understandable by children?
6.	How will you obtain consent from the parent or guardian of a child below 13 years of age, for the collection, use, or disclosure of the child's personal data?
7.	If you are collecting personal data for age assurance purposes, are you collecting the minimum amount of personal data necessary for those purposes?
Collection, use, and disclosure of personal data	
8.	Is your collection, use, or disclosure of the child's personal data reasonable?
9.	If you provide non-account-based services and are profiling children: • Will you be using anonymous or de-identified data to create the profile? • Will you be using the child's profile to target harmful content at the child?
10.	Have you ensured that the account information of children is not made public and searchable by default?

11.	Does your product or service make use of geolocation? If so: • Are you able to use approximate location data instead of precise location data? • Are you able to collect location data only when your product or service requires such data, rather than to be automatically collected continuously? • Are you collecting the minimum amount of geolocation data necessary for the purposes? • Does your product / service clearly indicate when geolocation is enabled and disabled? • Are the geolocation function(s) disabled by default so that precise location data is not automatically collected when a product or service is first used?
Protection of personal data	
12.	What measures will you put in place to protect the child's personal data?
13.	Have you implemented the Basic and Enhanced Practices listed in the PDPC's Guide to Data Protection Practices for ICT Systems, where applicable?
Data breach notification	
14.	Are you collecting personal data that, in the event of a breach, would result in, or be likely to result in, significant harm to the child concerned?
15.	Are there processes in place to ensure that the child, and the child's parents or guardians, are promptly notified in the event of a notifiable data breach?