5 April 2024

Singapore PDPC Issues New Guidelines on Children's Personal Data

The Personal Data Protection Commission (PDPC) of Singapore has published new Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment ("**Guidelines**") on 28 March 2024. These Guidelines aim to enhance data protection for children and ensure compliance with the Personal Data Protection Act (PDPA).

Who do the Guidelines apply to?

The Guidelines apply to organisations offering online products and services likely to be accessed by children, including:

- Social media services, as defined in the Broadcasting Act 1994;
- Educational technology (EdTech) products;
- Online games;
- Smart toys and devices.

Parts of the Guidelines also apply to data intermediaries.

What are the key principles?

The Guidelines recognise that children's personal data is sensitive and deserve a higher standard of protection under the PDPA. They explain how organisations can meet their statutory data protection obligations when dealing with children's personal data.

1. **Clear communication**[1]: Adopt age-appropriate language and media when communicating with children regarding the use of their data. For example, visual and audio aids will be more helpful than wordy policy documents.

2. **Age for consent**[2]: Organisations can obtain direct consent from children aged 13 and above unless they have reason to believe the child does not have sufficient understanding to give valid consent. Parental consent is mandatory for children under 13.

3. **Reasonable purposes only**[3]: Process children's personal data for reasonable and clearly defined purposes only, such as delivering age-appropriate content. Unreasonable purposes include targeting children with harmful or inappropriate content.

4. **Data minimisation**: Collect and retain only the minimum amount of children's personal data necessary for the organisation's reasonable purposes. For example, organisations should not build user profiles from children's information if it is not necessary.

5. **Age verification**: Organisations can implement age assurance methods, such as age verification or estimation, to tailor their data collection and use practices for compliance with the Guidelines and to implement relevant safeguards for child users, such as to ensure only age-appropriate content is accessible by users. These methods should be implemented at appropriate juncture(s), and not only at the account sign-up stage.

---

[1] *Pursuant to Section 20 of the PDPA, organisations must give individuals information about the types of personal data that will be collected and processed, and of the purposes for which their personal data is collected, used, and disclosed.*

[2] *Pursuant to Section 13 of the PDPA, valid consent is required for the collection, use, and disclosure of personal data.*

[3] *Pursuant to Section 18 of the PDPA, organisations may collect, use, or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.*

6. **Reconsider geolocation data**: While geolocation data alone may not be considered personal data, organisations should be mindful that combined with other identifiers, it can become so. The Guidelines recommend a data minimisation approach for children's personal data, such as disabling geolocation by default or collecting approximate locations only.

7. **Enhanced security measures**[4]: Organisations (including data intermediaries) handling children's data must implement appropriate security measures to protect such data, aligned with the PDPC's Guide to Data Protection Practices for ICT Systems. This is a nod to the sensitive nature of children's personal data.

8. **Conduct impact assessments**: Conducting Data Protection Impact Assessments (DPIA) is recommended, particularly before launching online products or services likely to be accessed by children.

9. **Who to notify in a data breach event**[5]: In the event of a notifiable data breach impacting children, notification must be made to both the child (in age-appropriate language) and their parents/guardians. If the organisation does not have contact details of the parent/guardian, it should advise the child to pass on the notification.

What should organisations do now?

Organisations should first consider whether the new Guidelines apply to them. If so, they should consider conducting a DPIA in accordance with the Guidelines, review their current data collection and use policies, practices, and agreements, and improve them if necessary, to ensure compliance. This will enable organisations to protect children's data and mitigate potential risks associated with non-compliance with the PDPA.

For queries or more information, please contact:

Wilson Wong
Director
wilson.wong@amicalaw.com
(65) 6303 6213

Geraldine Tan
Director
geraldine.tan@amicalaw.com
(65) 6303 6231

Anna Toh
Director
anna.toh@amicalaw.com
(65) 6303 6234

---

[4] *Pursuant to s 24 of the PDPA, organisations must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, or use, and loss of storage mediums or devices on which personal data is stored.*

[5] *Pursuant to s 26D of the PDPA, organisations must notify the PDPC no later than 3 days after assessing that a data breach is a notifiable data breach, and on or after notifying the PDPC, notify the affected individual.*

We wish to express our thanks to Joan Soo, our practice trainee, for her contributions to this update.