PDPC's Public Consultation on the Proposed Advisory Guidelines on Children's Data

31 August 2023

Tanglin Trust School Ltd

95 Portsdown Road,

Singapore 139299

DPO:

Ling Guan Heng

COO/CFO

Ling.guanheng@tts.edu.sg

Data Protection Committee

Lyssa Caneiro

Risk and Compliance Director

Lyssa.caneiro@tts.edu.sg

Lee Chin Peng

Director of Technology

ChinPeng.Lee@tts.edu.sg

Lena Chan

Corporate Legal Director

Lena.chan@tts.edu.sg

As an Education establishment Tanglin Trust School collects student personal information with the consent of parents until the student is 18 years old. The information is used to provide the services of education, safeguarding, sports, school trips & meals and disclosed to relevant external third parties in the provision of these services. Guidelines on Children's data protection especially in Education would be very helpful.

Question 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?
Agree that it is important to have guidelines to ensure children and young people's personal and sensitive information is protected to keep them safe.

a. If the Guidelines are able to be clear on how to identify such products and services, in principle the same rules should apply as the rules used for products and services which are targeted at children. However this is an inherently difficult end to achieve – children have access to all sorts of goods and services, further, in many instances data controllers have no way of knowing that the data subject is a child - then such an application of the Guideline is likely to be overly onerous simply by the difficulty in application.
b. Agree as it would be incongruous that the Guidelines applied to controllers but not to intermediaries.

Question 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?
From the point of view of a school, these include - providing education services, monitoring student's academic performance, identifying learning difficulties, monitoring student's behaviour for safeguarding and providing counselling or child protection support, providing first aid and health services, preventing students from engaging in risk taking behaviours, organising events, arranging music & sports co-curricular activities, academic and adventurous trips, providing food services, providing travel to and from school, alumni purposes, record keeping, and assisting students who are changing schools.

Question 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?
Use of age-appropriate books, drawings, cartoons, e-learning applications, movies, YouTube videos, games, creating plays, using toys and other physical and tactile models.

Question 4: How should organisations minimise the collection, use, and disclosure of children's personal data?
The overarching rule that an organisation should collect/use/disclose only what personal data it needs to would apply to children's data and that should be a sufficient standard.

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?
Protect the data collected, preferably in electronic format and limit access with 2FA protection, ensure staff are trained on Data protection, keep data limited to those who need to know, and users have passed pre-employment child protection checks to support access to this information.
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?
It depends on the purpose of use. We would want geolocation on if the information is to ensure the person is in the correct country and should have access to the site and content, and to confirm the account has not been hacked and used by a person in a different location. If the person or their assets are missing, and we need to know if they are safe, or their assets have been stolen and used without their legal permission.

Question 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?
DPIA should be conducted if an organisation is launching electronic services or products that could result in addiction or harm to the participants, e.g., games which include purchases, violence, targeting vulnerable others, if the application could create mental health concerns, or if the application has potential to be used for bullying or grooming by bad actors.
The organisation should consider normal usage factors and the abuse of usage by people with intent to cause harm to children and young people and how the product can be designed with protection measures from the start.

Question 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?
Whilst in safe environments with sufficient scaffolding, children of 13-17 should have sufficient understanding, e.g., the school has validated the content and students subscribe to the service using their school account. However, there are situations where products become available which are meant to appeal to that age group, but the purpose of use or abuse is not obvious. Hence, there should be oversight by parents and trusted adults to prevent children of that age group from being targeted and getting into financial problems or having access to inappropriate or harmful content.

If unsupported, children aged between 13-17 are generally not sufficiently mature and knowledgeable to provide consent with respect to their personal data. Understanding use of personal data requires context, which children by reason of their fewer years of experience, might not possess.

Question 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?

The guide is very comprehensive and useful for all organisations. We consider that the measures in the Guide are adequate protection for children's data and note that some of the Enhanced practices are already a challenge to implement.

Question 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?

When data breached contains addresses or contact information and there are safeguarding concerns, or the breached information could lead to potential harm from other adults or children if information was published, or risky behaviours that the child has been involved in could result in legal action or embarrassment, it is essential that the information is protected to the highest levels and any breach is notified.

Nonetheless, the data breach notification should be sent to the person who gave the consent. So where the organisation obtains consent in relation to the child's data primarily from the parent, then the notification should go to the parent. It should not be necessary to send the child a separate notification.

However if consent is given by the child, for eg. in the case where a child 13 and above is determined is able to give good consent, then requiring the parent to be notified might not be possible as the organisation might not have collected the contact details of the parent at all. If it is considered that children need their parents to protect them from the consequences of a breach of their personal data likely to result in significant harm, it should also follow that children need their parents to consent on their behalf.

Additional Feedback: PDPA First Schedule, Second Schedule, Fifth Schedule

We seek indulgence to provide feedback on another matter.

As a school there are occasions when safeguarding concerns about students require sharing the information without the consent of the children or parents. For example when the concern arises from a parent's ill-treatment of the child, and the child is transferring schools whether in Singapore or outside Singapore, the information should be shared with the child's next school so that they can help keep the child safe. Safeguarding information will invariably include personal data, and currently the school is constrained from sharing by personal data laws as well as the laws on confidentiality.

The current exceptions in the PDPA do not apply to protect the school in these circumstances because most situations although serious, are not an emergency, and neither is there an issue with obtaining consent in a timely way. Schools should be protected when acting in the best interests of the child.

A related issue is that a parent has a right to request access personal data of his child even if it is safeguarding information which may put the child at risk if the parent obtains the information. For instance where a child discloses to the school an abuse by the parent and the child is likely to suffer harm if the parent comes to know of the child's disclosure, the exceptions to Access rights do not allow the school to refuse an access request from a parent in most cases. There could also be occasions where parents have custody issues or where there are child protection concerns so it is not appropriate to provide access to all the data held about subjects or their children, and also not to comply with deletion requests. Legal protection may be required for these situations.

On retention, there could also be occasions when children may want access to information once they are grown adults, more mature and finally able to process the harm that was done to them when they were children. There may have been conversations and observations that would have been documented by the school through pastoral support and counselling that they need to access, or they may raise issues years later and want to know more about people involved. Schools have to address these situations in data protection and retention guidelines. Although the PDPA does not stipulate timelines and does allows organisations to justify their retention decisions, the Guidelines state clearly that retention for "just in case" is not allowed. Safeguarding information which does not disclose a crime on its own, can still constitute critical evidence of abuse and in our humble opinion, schools should be allowed to retain such information just in case the student wants to pursue his rights when he is older.