PAP Community Foundation

[2019] SGPDPC 6

Yeong Zee Kin, Deputy Commissioner — Case No DP-1807-B2434

Data Protection – Protection obligation – Unauthorised disclosure of personal data – Insufficient security arrangement

23 April 2019.

Background

1 The Organisation provides a range of services, including pre-school kindergarten services and senior care services. The central issue to this case, in so far as it is related to the Personal Data Protection Act 2012 ("**PDPA**"), is whether the Organisation had made reasonable security arrangements to protect the personal data of the students and students' parents that it had in its possession and control at the material time.

Material Facts

2 One of the many preschools under the Organisation's management is the Sparkletots @ Kampong Chai Chee centre (the "**preschool**"). In the course of the year, the preschool would organise various school trips, sometimes with the participation of the parents. In preparation for these trips, the preschool would collect the parents' personal data (including NRIC numbers) to allow for verification of the parents' identity on the day of the trip.

3 The present investigations arise from one such school trip. A few days before the trip was scheduled to take place, a teacher at the preschool sent a photograph of a consolidated attendance list to a "WhatsApp" chat group, reminding parents of the upcoming school trip. The attendance list contained personal data relating to the 15 students in that particular class and their parents, and included the contact numbers and NRIC numbers of five of the parents (the "**Personal Data**"). The "WhatsApp" chat group comprised of the parents of students from that class.

4 The teacher who sent the photograph of the attendance list quickly deleted it after being alerted to the disclosure of personal data by one of the parents within the group chat. That same parent later lodged a complaint with the Personal Data Protection Commission ("**PDPC**"). The PDPC thereafter commenced investigations into the incident.

The Deputy Commissioner's Findings and Basis for Determination

The Relevant PDPA Provisions

5 In respect of this matter, the relevant provision is section 24 of the PDPA. Section 24 requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

Preliminary Issues

6 It is not disputed that the Personal Data is "personal data" as defined in section 2(1) of the PDPA. There is no question or dispute that the Organisation falls within PDPA's definition of an "organisation". There is also no dispute

that the Personal Data was, at all material times, in the Organisation's possession and under their control and that the Organisation was responsible for the Personal Data.

7 The key issue is therefore whether the Organisation had protected the Personal Data in its possession and under its control by making reasonable security arrangements to prevent unauthorised access and similar risks.

The Organisation failed to make reasonable security arrangements

8 After a review of all the evidence obtained by PDPC during its investigation and for the reasons set out below, I am of the view that the Organisation had failed to make reasonable security arrangements to protect the personal data in its possession and control, and has thereby breached the Protection Obligation under section 24 of the PDPA. This breach is attributable primarily to the Organisation's lack of specific policies or procedures in place to guide its employees on the use, handling and disclosure of personal data, especially in the context of communicating with parents.

9 It bears noting that "security arrangements", as envisaged in section 24 of the PDPA, encompass physical, technical and administrative measures to protect personal data. Such measures include data protection policies and procedures that employees must comply with in the course of their work. "Reasonable" in section 24 implies that the security arrangements in place are commensurate with the nature and volume of the personal data that the organisation possesses and/or controls.

10 In this regard, the Organisation has about 360 Sparkletots Centres with about 43,000 children enrolled. By the very nature of its kindergarten/ preschool business, the Organisation collects, possesses, and handles a significant amount of personal data of minors and parents alike. The everyday frequency of interaction between its staff and the parents of the children under the Organisation's care indicates also that specific policies or training would reasonably be expected to be put in place in order to guide staff on the PDPA obligations that will undoubtedly be engaged during their day to day activities. In the course of their work, the Organisation's staff are more likely than not to be placed in situations where the use and disclosure of personal data is crucial to the discharge of their duties, as it was with the case of obtaining consent for and organising the school trip in question.

11 The Organisation has admitted that it did not have such specific policies or procedures in place to guide its employees on the use and disclosure of personal data in their communications with the parents of students enrolled at the organisations preschools. While it had a Data Protection Notice, this was a document that was intended to provide general information about how the Organisation handles personal data. It was meant for an external audience. It was not intended to provide detailed guidance to its teaching and other staff on how they should handle personal data in the course of their work. Since the Organisation handles personal data of its students and their parents, the omission to provide detailed guidance to its teaching and other staff is an obvious gap in its security arrangements. To my mind, the Organisation needs to provide guidance to its employees in the area of communications and transmission of documents containing personal data, such as *via* messaging applications. The absence of such policies and procedures meant that the Organisation had little assurance that its employees were consistently

performing their duties in a PDPA-compliant manner. This falls short of the standard of "reasonable security arrangements".

12 That said, the Organisation had provided PDPA training to its employees at the preschool, including the teacher who had disclosed the attendance list. While PDPA training raises employees' awareness of their obligations, this serves as a useful illustration that mere training alone cannot be a substitute for data protection policies and procedures in specific areas. Reasonable assurance against such incidents requires instituting and enforcing proper policies and procedures within an organisation, with training sessions acting as the medium to communicate such policies.

Conclusion

13 Based on the foregoing, I find that the Organisation has breached the Protection Obligation under section 24 of the PDPA.

14 Having found the Organisation to be in breach of section 24 of the PDPA, I am empowered under Section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

15 In determining the appropriate directions to be imposed on The Organisation, I have taken into account the following mitigating factors:

(a) The teacher in question acted swiftly in removing the Personal Data from the "WhatsApp" group; and

(b) The number of individuals impacted by the disclosure (15 students and 30 parents) was relatively small and the disclosure was constrained to the group of parents to whom the Personal Data pertained to.

16 To its credit, the Organisation also acted swiftly to address their inadequate policies – a response which, in my assessment, carries mitigating value. The following remedial actions taken by the Organisation have therefore been taken into account:

(a) Immediate suspension of all "WhatsApp" chat groups following the disclosure;

(b) Expedited the implementation of a set of "Social Media Policy / Whatsapp chat group rules" that was already under development when the breach occurred;

(c) Rolled out a suite of other policies across the Organisation including a "Document Retention Policy" and an "Information Security Policy"; and

(d) Undertook the development of a practical employee handbook and conducted refresher training for its employees.

17 Having considered all the relevant factors of the case, I am of the view that these remedial actions have sufficiently addressed the current gap in policies and practices relating to the handling of personal data by the Organisation's employees. I have therefore decided to issue a warning to the Organisation for breaching its obligations under section 24 of the PDPA, without further directions or imposing a financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
[FOR COMMISSIONER] FOR PERSONAL DATA PROTECTION