**DECISION OF THE PERSONAL DATA PROTECTION COMMISSION**

**Case Number: DP-1605-B0028**

**In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012**

**And**

**National University of Singapore**

**... Organisation**

**Decision Citation: [2017] SGPDPC 5**

**GROUNDS OF DECISION**

26 April 2017

1. A student of the Organisation had complained to the Personal Data Protection Commission (the "**Commission**") that a URL link that was being circulated for the Organisation's orientation camp had disclosed (without authorisation) the personal data of student volunteers from the College of Alice and Peter Tan ("**CAPT**"). CAPT is a residential college of the Organisation.

2. It was found that by following the URL link, one could access an online Excel spreadsheet containing the full names, mobile numbers, matriculation numbers, shirt sizes, dietary preferences, dates of birth, dormitory room numbers, and email addresses (the "**personal data set**") of approximately 143 student volunteers. The student matriculation number is a unique student identification number issued by the Organisation. The matriculation number to a student is, in a limited sense, like an NRIC number to a Singapore citizen and permanent resident, in that it is required for various school activities, such as accessing online library resources, or for the submission of examination scripts.

3. Based on the complaint that was made, the Commission proceeded to investigate into an alleged breach by the Organisation of the protection obligation under Section 24 of the Personal Data Protection Act 2012 ("**PDPA**"). The following sets out the Commission's findings following its investigations into the matter.

## A. MATERIAL FACTS AND DOCUMENTS

4. The CAPT Freshman Orientation Camp ("**FOC**") is an annual event organised by student volunteers from CAPT for the freshmen matriculating into the Organisation. The FOC in the present case was for the year 2016.

5. The Organisation had designated several student leaders to take the responsibility for organising the FOC. As part of the process of organising the FOC, these student leaders would recruit other student volunteers to participate as counsellors and assist in the running of the FOC.

6. To get themselves organised, the student leaders created an online form using Google Forms[1] for the student volunteers to fill in their personal particulars. The particulars that were entered into the Google Forms were stored in a Google Sheets[2] spreadsheet (the "**Spreadsheet**"), which compiled all the particulars of the various student volunteers in a single spreadsheet.

7. The Spreadsheet was meant to be shared amongst the student leaders only, and not to the student volunteers, or anyone else. For the purpose of sharing access to the Spreadsheet, a URL link to the Spreadsheet was generated through Google Sheets by selecting the "Share with specific people" function, and this URL link was then shared amongst the student leaders. Only specified persons could access the Spreadsheet as the URL link to the Spreadsheet required a user to first log in with his or her Google account.

8. While the Spreadsheet was initially circulated to specified people (i.e. the student leaders), at some point in May 2016, the Spreadsheet came to be circulated beyond the originally intended group. An unknown party, whether intentionally or otherwise, changed the setting on the Spreadsheet from "Share with specific people" to "Share using a link". As a result, any user who possessed the URL link could access the Spreadsheet, and all the personal data set of the student volunteers contained within.

9. Consequently, the personal data set was now exposed to those who had access to the URL link, which may have extended to persons beyond the Organisation itself.

---

[1] **Google Forms** – An online form creation application by Google. Users can create, edit and distribute the form easily, and save responses into a Google Sheet. See <https://www.google.com/forms/about/> for more information.

[2] **Google Sheets –** An online spreadsheet application by Google, which enables users to create, edit and share spreadsheets. Sharing spreadsheets allows multiple users to edit the same spreadsheet at the same time. See <https://www.google.com/sheets/about/> for more information.

## B. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

10. The Organisation has not shied away from its responsibility for the data breach incident, and has confirmed that the FOC was an event that it had sanctioned. The Organisation has mentioned that any act done in the name of CAPT, which was authorised by the Organisation, was an act done in the name of the Organisation.

11. Given that the FOC activities were carried out in the Organisation's name, the Organisation is ultimately responsible for ensuring that the personal data of its students is adequately protected pursuant to Section 24 of the PDPA.

12. In light of the events of this case, the relevant issue for determination is whether the Organisation had indeed complied with Section 24 of the PDPA.

Whether the Organisation was in breach of Section 24

13. In its response to the Commission during investigations, the Organisation did not dispute the fact that the data breach had occurred. However, the fact that the data breach occurred is not necessarily indicative of a contravention of the PDPA. Rather, it is necessary to consider whether the Organisation's safeguards that were in place at the material time were adequate having regard to the volume and type of personal data in question, and whether the safeguards were reasonable in the circumstances.

*The Organisation's security arrangements at the material time*

14. Security arrangements to protect personal data may take various forms, including administrative, physical, technical measures or a combination of these. According to the Organisation, it had, at the material time, implemented administrative safeguards, in the form of data protection training and guidelines, to adequately protect the personal data set in its possession and under its control:

    (a) Data protection training: The Organisation conducted classroom training in or around 2014 on the relevant data protection obligations that apply to the collection, use and disclosure of personal data for selected students who were likely to hold leadership roles. However, it would appear that the classroom training did not carry over to 2015. In 2015, the Organisation had instead provided all its students with access to e-training on the PDPA. This e-training appeared on the list of trainings available on the Integrated Virtual Learning Environment ("**IVLE**") portal

such that when students logged into the system, the e-training option would be visible to them.

(b) Data protection guidelines: The Organisation issued guidelines for the students organising various events in the name of the Organisation to ensure that all student activities complied with the Organisation's regulations. These guidelines were adapted to become the *CAPT Event Planning Guidelines for Student Groups* ("**CAPT Guidelines**"). The CAPT Guidelines contained a section titled "Responsible Usage and Access of Personal Data". Students in charge of planning activities in the name of the Organisation who collected personal data, such as "*name, Matric No., email address, HP number*", were reminded to "*observe proper use and access to prevent potential data leakage and unauthorized/accidental access*."

*The Organisation did not provide adequate training for the student leaders*

15. Although the Organisation had in place general policies and guidelines for the protection of personal data, when it came to the security arrangements on the ground, the Organisation did not have any formalised data protection training in place to train and equip its students with the mind-set, knowledge, skills and tools to protect personal data.

16. While the Organisation had made the e-training programme available on IVLE, the Organisation did not make it compulsory for all the student leaders of the FOC to undergo the e-training. In any case, the Organisation confirmed that none of the student leaders had undergone the e-training prior to the commencement of the FOC in 2016, even though the student leaders were involved in the handling of the personal data of other students.

17. With regard to classroom training, it appeared to have been held only once in 2014, and was only for the benefit of selected students. Although the Organisation claimed that it had plans to make this classroom training an annual event, no such plans had materialised by the time of the FOC in 2016.

18. In this regard, there was effectively no data protection training provided to the student leaders of the FOC in 2016.

19. By the Organisation's failure to provide adequate training for the student leaders before they handled personal data, this increased the risk of a data breach occurrence. Even if a student leader had some knowledge of the PDPA, how that translated into the actual practice of protecting personal data was something that the Organisation would not be able to ensure.

20. We pause to set out how training falls as a consideration for ensuring adequate protection of personal data under the PDPA.

*Training as a type of security arrangement*

21. Data protection training may fall under two separate data protection obligations – the openness obligation (Sections 11 and 12, PDPA) and the protection obligation (Section 24, PDPA). An organisation that is subject to the openness obligation is required to communicate to its staff information about its policies and practices, pursuant to section 12(c) of the PDPA. This communication of the data protection policies may necessarily involve some form of staff training.

22. While the openness obligation may not extend to student leaders who are not members of staff, data protection training may also be seen as an administrative security measure that is necessary for compliance with the protection obligation. In its advisory guidelines, the Commission provided examples of administrative security measures such as the conducting of "*regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data*".[3] [Emphasis added.]

23. In the UK, administrative or organisational security measures may encompass relevant and appropriate training of staff on the data protection obligations of the organisation, especially for employees that collect, use or disclose personal data.[4] In describing the management and organisational measures that an organisation should put in place, the UK's Information Commissioner's Office highlighted the importance of staff training and stated that:

> "*[i]t is vital that your staff understand the importance of protecting personal data; that they are familiar with your organisation's security policy; and that they put its security procedures into practice. So you must provide appropriate initial and refresher training…*"[5]
>
> [Emphasis added.]

24. Similarly, in Canada, the Office of the Information & Privacy Commissioner for British Columbia expressly stated in the case of *Park Royal Medical Clinic* that

---

3 PDPC, *Advisory Guidelines on Key Concepts in the PDPA* (revised 15 July 2016) <https://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines/main-advisory-guidelines#AG1> at [17.5].

4 Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (OUP, 4th Ed, 2015) at p 126.

5 Information Commissioner's Office, *Information security (Principle 7)* (25 October 2016) <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/> at 4.

"*administrative security, which encompass policies and training regarding privacy is another important component*" of the obligation to make reasonable security arrangements.[6] In another case, the Office of the Privacy Commissioner of Canada ("**OPC**") explained that whilst security policies and procedures are essential, they are not in themselves sufficient to protect personal information; the effectiveness of security safeguards depends on the organisation's:

> *"[d]iligent and consistent execution of security policies and procedures [which] depends to a large extent on ongoing privacy training of staff and management, so as to foster and maintain a high organizational awareness of informational security concerns"*.[7]

25. In a separate investigation, the OPC further clarified its position and stated that security policies and practices are only effective when "*properly and consistently implemented and followed by employees*".[8]

26. In Hong Kong, the Office of the Privacy Commissioner for Personal Data stated in its Code of Practice on Human Resource Management that employees "*play the principal role in implementing an employer's policies on the security of personal data*". Organisations should take reasonably practicable measures to ensure that employees handling personal data are trained to observe the personal data privacy policies, exercise due diligence in the application of those policies, and are subject to procedures designed to ensure their compliance with those policies.[9] This statement is in line with Principle 4 of Hong Kong's *Personal Data (Privacy) Ordinance*, i.e. security of personal data.[10]

27. Overall, the foreign data protection authorities all seem to agree that the data protection training provided by an organisation may constitute a type of administrative or organisation security measure, and that this training has an impact on the proper implementation of that organisation's data protection policies and practices.

---

6 *Order P15-01: Park Royal Medical Clinic* 2015 BCIPC 20 <https://www.oipc.bc.ca/orders/1783> at [58].

7 *PIPEDA Case Summary #2008-395: Commissioner initiates safeguards complaint against CIBC* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2008/pipeda-2008-395/>, second bullet point in the "Lessons Learned" section at p 1.

8 *PIPEDA Report of Findings #2016-005: Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/> at [74].

9 Office of the Privacy Commissioner for Personal Data, Hong Kong, *Code of Practice on Human Resource Management* (April 2016) (First Revision) <https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf> at [1.4.1].

10 *Personal Data (Privacy) Ordinance* (Chapter 486) (Hong Kong) Schedule 1, Principle 4.

28. The above positions are useful in our case here. In the Commission's view, a formalised data protection training for the student leaders for the FOC would be beneficial in several aspects. Not only would it inform the student leaders of the PDPA, but it would also sensitise them to their personal data protection obligations. Further, it also trains the students on the practices to be adopted, and not just pay lip service to the PDPA obligations, or to the Organisation's policies. Additionally, it may provide some guidance for students to go about their tasks when it comes to handling personal data.

*Organisation's breach of Section 24 of the PDPA*

29. As mentioned above, the Organisation did not have in place any formalised training for the student leaders, even though it was reasonably foreseeable that they would be handling personal data in the course of organising the FOC.

30. The FOC was an event that involved many students, and would potentially involve the handling of many students' personal data. The Organisation ought to have at least ensured that the student leaders organising and running the FOC had the proper training to deal with and protect the personal data that they will handle. Moreover, since the FOC was an event that takes place annually, the Organisation could have anticipated and planned for some form of training to be provided to the student leaders that were handling the personal data.

31. Since the FOC was an annual event, the training that can be provided can also be customised to the FOC and the data processing activities that will foreseeably be carried out. Such customisation could be based on considerations such as (a) to whom the training should apply (i.e. confined to just the student leaders or extending also to student volunteers); (b) the most effective way of disseminating best practices to all who may come into contact with personal data; and (c) the frequency and timing of such training. To be clear, the Commission is not setting down any rule that mandates formalised classroom training. The Organisation should adopt a mode of training that it considers to be effective and expedient, having regard to these factors.

32. In this case, it was not enough for the Organisation to rely solely on the CAPT Guidelines in order to protect personal data. Apart from the fact that it was unclear whether the student leaders were fully apprised of the CAPT Guidelines, the CAPT Guidelines did not necessarily translate into actual processes that would enable the student leaders to comply with the data protection obligations in practice. Proper guidance is not easily substitutable or replaceable by general guidelines that an organisation may set.

33. In view of the fact that the Organisation did not put in place adequate training for the student leaders, the Commission finds that the Organisation failed to make reasonable security arrangements to protect the personal data in its possession and/or under its control and is in breach of Section 24 of the PDPA.

## C. THE COMMISSION'S DIRECTIONS

34. The Commission is empowered under Section 29 of the PDPA to give the Organisation such directions as it deems fit to ensure the Organisation's compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million as the Commission thinks fit.

35. In assessing the breach and determining the directions to be imposed to the Organisation in this case, the Commission took into account the following factors:

(a) a significant number of individuals (approximately 143 students) were affected by the data breach incident;

(b) the potential adverse consequences from a misuse of the student matriculation number by other persons. For example, passing off as a student to carry out identity theft, or even carrying out pranks or nuisances in the student's name. It was however noted that the student matriculation number is used as an identifier for the duration of the student's undergraduate or postgraduate course and not for an extended period of time; and

(c) the Organisation was cooperative with the Commission and forthcoming in its responses during the Commission's investigation.

36. Pursuant to Section 29(2) of the PDPA, and having completed its investigation and assessment of this matter, the Commission is satisfied that the Organisation was in breach of the protection obligation under Section 24 of the PDPA. The Commission has decided to issue directions to the Organisation, pursuant to Section 29 of the PDPA, in respect of the Organisation's breach of Section 24 of the PDPA.

37. The Commission had provided its preliminary grounds of decision and directions to the Organisation directing the Organisation to essentially (a) implement mandatory training for its student volunteers within 60 days and (b) provide an update to the Commission of the training arrangements it had put in place.

38. The Organisation's Data Protection Office accepted the Commission's findings but made representations in respect of the preliminary directions, requesting:

(a) for a longer duration of 120 days for the Organisation to fully implement the necessary training modules for its student leaders, which will apply to not just future freshman activities, but for other activities sanctioned by the Organisation; and

(b) that the direction for mandatory training should refer to "student leaders", which should take the following suggested meaning: "*any undergraduate or post graduate student of [NUS] who has been appointed or is part of any committee tasked to organize any event/activity officially approved or sanctioned by [NUS]"*.

39. The Commission has considered and accedes to the representations. While the Commission generally has the power to impose such directions as it deems fit in the circumstances, the Commission is prepared to consider representations from organisations on the grounds of decision and the form of directions to be issued, especially since directions ought to be adapted or customised to their operations or practices to be *effective* in addressing the particular shortcomings that had been identified during investigations. In the present case, the Commission accepts the representations since they do not detract from the key principles, functions and purposes of the Commission's grounds of decision and directions.

40. However, the Commission clarifies that its directions are tailored to enable the Organisation to effectively address the shortcomings that had been identified during investigations. In this regard, while the Organisation has been directed to put in place mandatory training for student leaders of officially approved or sanctioned activities, that does not mean that for other types of activities, there is no need for the Organisation to put in place policies, create awareness or provide voluntary training. The PDPA imposes a free standing and continuing obligation on the Organisation to ensure that its policies are effective in implementing the requisite standard of personal data protection. It behoves the Organisation to consider whether, beyond the directions issued in this case, any further arrangements are necessary.

41. Having carefully considered all the relevant factors of this case, the Commission hereby directs that:

(a) the Organisation to, within 120 days from the date of the Commission's directions:

(i) design training (including online training and dissemination of training materials) that would address personal data protection in the context of the collection and processing of personal data for student events and of the resulting interaction;

(ii) make arrangements for such training to be mandatory for any student leader. For the avoidance of doubt, a student leader is defined as any undergraduate or post graduate student of the Organisation who has been appointed or is part of any committee tasked to organize any event or activity officially approved or sanctioned by the Organisation;

(iii) make other arrangements as would be reasonably required to meet the objectives in 41(a)(i) and 41(a)(ii); and

(b) by no later than 14 days after the above action has been carried out, the Organisation shall, in addition, submit to the Commission a written update providing details on the arrangements for the training for student leaders managing personal data for student events officially approved or sanctioned by the Organisation.

**YEONG ZEE KIN**
**DEPUTY COMMISSIONER**
**PERSONAL DATA PROTECTION COMMISSION**