Singapore Taekwondo Federation

[2018] SGPDPC 17

Tan Kiat How, Commissioner — Case No DP-1705-B0810

Data Protection – Openness obligation – Failure to designate one or more persons to be responsible for ensuring that the Organisation complies with the PDPA

Data Protection – Openness obligation – Lack of data protection policies and practices

Data Protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

22 June 2018.

Background

1 This matter involves the Singapore Taekwondo Federation (the "**Organisation**"), a society registered with the Registry of Societies that is responsible for promoting, supporting, and developing taekwondo-related programmes and activities in Singapore.

2 Since 2015, the Organisation has been posting, on an annual basis, PDF documents which contain the names and schools of students who are participants of the Annual Inter-School Taekwondo Championships ("**Championships**") on the Organisation's website which is accessible to the general public. It was represented by the Organisation that the purpose of

uploading the PDF documents on its website was to enable students to verify their participation in the Championships.

3 On 30 May 2017, a complaint was lodged by a member of the public ("**Complainant**") with the Personal Data Protection Commission ("**Commission**"), alleging that there was an unauthorised disclosure of the NRIC numbers of 782 students who were participants of the 2017 Championships. Whilst the NRIC numbers, within the PDF documents, were set out in columns that were minimised, and, hence, not immediately visible, there was an unauthorised disclosure of these NRIC numbers when the Complainant subsequently copied and pasted the contents of the PDF documents on to another document.

4 The Commissioner sets out below his findings and grounds of decision based on the investigations carried out in this matter.

Material Facts

5 On 19 May 2017, the Complainant chanced upon the PDF documents on the Organisation's website, which contained the names and schools of students who were participants of the 2017 Championships.

6 The NRIC numbers of the students were not immediately visible to the Complainant in the PDF documents, as the NRIC numbers were set out in columns which were minimised. Nevertheless, when the Complainant copied and subsequently pasted the contents of the PDF documents on to another document, he was able to view the NRIC numbers of the students. The Complainant proceeded to inform the Organisation of this unauthorised disclosure of the students' NRIC numbers via email on 19 May 2017.

7 As the Complainant did not receive any response from the Organisation, he proceeded to lodge a complaint with the Commission on 30 May 2017. Upon receiving the complaint, the Commission commenced an investigation into this matter.

8 On 31 May 2017, after the Organisation was notified by the Commission of the unauthorised disclosure of the students' NRIC numbers, the Organisation removed the PDF documents from its website. The Organisation represented that it had also taken steps to contact Google to remove the cache, as well as instructed its staff to delete the relevant information in question before uploading any documents on to the Organisation's website.

9 During the course of the Commission's investigation, the Organisation made the following representations in relation to its process of handling the personal data of the students intending to participate in the Championships. Firstly, it would receive an encrypted Excel spreadsheet containing the personal data of students intending to participate in the Championships, including their names, NRIC numbers, dates of birth, gender, school, class, taekwondo grade, names of taekwondo instructors and clubs, from the Physical Education Sport Education Board of the Ministry of Education ("**MOE**").

10 After receiving the encrypted Excel spreadsheet, the Organisation's Head of the Tournament Department ("**Tournament Head**") would typically proceed to rearrange the students' personal data into programme lists and bout sheets using Microsoft Excel. The Tournament Head asserted that in relation to the Excel spreadsheets containing the students' personal data, he would "hide" their NRIC numbers, before converting the Excel spreadsheets into PDF documents.

11 The Tournament Head describes the process as follows:

> "I will copy and paste the names, NRIC numbers, and schools into a new excel spreadsheet. I will then hide the NRIC numbers and then add in the programmes into the new excel spreadsheet. I have been doing this since 2015.
>
> Thereafter, I will send the new excel spreadsheet with the names, schools, programme list and hidden NRIC numbers to [redacted] who will then convert it into a PDF list for uploading onto STF's website. She also has been doing this since 2015 but she does not know that I simply hide the NRIC numbers".
>
> [Emphasis added.]

12 The investigation carried out by the Commission sought to verify the assertion made by the Tournament Head. A check on the internet, including the website of Adobe Systems Incorporated, the proprietor of the Adobe PDF software, did not reveal the reappearance of "hidden" contents when copied to a separate Microsoft Word or Excel document ("**Alleged Bug**") to be a known issue or function.

13 In addition, officers of the Commission had conducted tests to replicate the result of the Alleged Bug. The officers of the Commission first copied the PDF documents in question found on the Organisation's website to a newly created Microsoft Word document and found that the columns which were not visible on the PDF documents appeared when copied to the Microsoft Word document. This verified the Complainant's assertion. However, when the officers of the Commission created a new Excel spreadsheet with properly hidden columns, this Alleged Bug did not occur. Subsequently, the officers of the Commission discovered that this issue would only occur if the columns were minimised instead. In other words, if the columns in an Excel spreadsheet were minimised instead of hidden, and the Excel spreadsheet were to be converted into PDF format, then the contents of the minimised columns would reappear when the PDF document was copied onto a Microsoft Word or Excel document.

14 Based on the foregoing, the Commissioner finds that the columns in the Excel spreadsheet prepared by the Tournament Head were not hidden but merely minimized.

15 In relation to the reason for purportedly hiding (but actually minimizing) the column with NRIC numbers in the Excel spreadsheet, the Organisation represented that this was for the sake of convenience in submitting the results of the Championships to participating schools. Following the conclusion of the Championships, participating schools would typically request for the name lists of the medalists and the results of the Championships, which would have to contain the students' NRIC numbers, so as to allow the schools to verify and present colour awards to their students.

16 The Organisation conceded that it was not aware that there were columns which had been minimised in the PDF documents, such that the NRIC numbers in these columns appeared when the contents of the PDF documents were copied and pasted to another document.

17 In addition, the Organisation admitted during the course of the investigation that it was not aware of the Personal Data Protection Act 2012 ("**PDPA**"). Consequently, the Organisation did not appoint a data protection officer ("**DPO**"), nor did it implement any policies or practices necessary for it to meet its obligations under the PDPA.

Findings and Basis for Determination

18 The issues for determination are as follows:

(a) whether the Organisation had complied with its obligation under section 11 of the PDPA to designate one or more persons to be responsible for ensuring that the Organisation complies with the PDPA;

(b) whether the Organisation had complied with its obligation under section 12 of the PDPA to develop and implement policies and practices that are necessary for the Organisation to meet its obligations under the PDPA; and

(c) whether the Organisation had complied with its obligation under section 24 of the PDPA to implement reasonable security arrangements to protect personal data in the Organisation's possession or under the Organisation's control.

19 At the outset, although the Tournament Head represented during the investigation that the Organisation is managed mostly by a team of volunteers, pursuant to section 53(1) of the PDPA, the Organisation would be responsible for its employees (which includes volunteers[1]) actions which are engaged in the course of their employment[2].

20 In addition, the NRIC numbers that were disclosed constitutes personal data as defined in section 2(1) of the PDPA, as every single student in the PDF documents could be identified from the NRIC numbers disclosed. Accordingly, the Organisation would be subject to the data protection obligations under Parts III to VI of the PDPA.

---

1 Section 2(1) of the PDPA.

2 Section 53 of the PDPA read with section 4(1)(b) of the PDPA.

Nature of personal data

21 As a preliminary issue, the Commissioner first considered the nature of the personal data in this matter.

22 The personal data disclosed NRIC numbers which, according to the Commission's Advisory Guidelines on Key Concepts in the Personal Data Protection Act[3] ("**Key Concepts Guidelines**") and the Guide to Basic Data Anonymisation Techniques[4] ("**Anonymisation Guide**"), constitute a data attribute that is assigned to an individual for the purposes of identifying the individual and, on its own, identifies an individual.[5] The Commission's Advisory Guidelines on the PDPA for Selected Topics[6] ("**Selected Topics Guidelines**") also recognise that "*NRIC numbers are of special concern to individuals as they are unique to each individual*" (emphasis added).[7]

23 In addition, the NRIC numbers that were disclosed were the NRIC numbers of students, minors who were less than 21 years of age. The Selected Topics Guidelines recognise that certain considerations may arise in this regard, including that "*there is generally greater sensitivity surrounding the treatment of minors*" (emphasis added).[8] Therefore, good practices in protecting minors' personal data include, amongst other things, placing "*additional safeguards*

3 Revised on 27 July 2017.

4 Published on 25 January 2018.

5 Anonymisation Guide at [3.1] and Key Concept Guidelines at [5.9].

6 Revised on 28 March 2017.

7 Selected Topics Guidelines at [6.1].

8 Selected Topics Guidelines at [8.12].

(*cont'd on next page*)

against [the] unauthorised disclosure of, or unauthorised access to, [the] personal data of minors" (emphasis added).[9]

24 A similar approach in respect of minors' personal data has been adopted in several other jurisdictions. In Canada, the Office of the Privacy Commissioner of Canada ("**OPC**") has expressed that it "*has consistently viewed personal information relating to youth and children as being particularly sensitive and must be handled accordingly*" (emphasis added).[10]

25 In the United Kingdom, the Information Commissioner's Office ("**ICO**") has taken the view that "*children need particular protection when [an organisation is] collecting and processing their personal data*" (emphasis added) and if an organisation processes children's personal data, the organisation "*should think about the need to protect them from the outset, and design [the organisation's] systems and processes with this in mind*".[11] The ICO has also expressed that there are "*important additional considerations that need to [be taken] into account when [an organisation's] data subject is a child*" (emphasis added).[12]

---

9 Selected Topics Guidelines at [8.12].

10 OPC, Guidance for businesses that collect kids' information at <https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/gd_bus_kids/>.

11 ICO, Guide to the General Data Protection Regulation (22 March 2018) at <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> at p. 155.

12 ICO, Consultation: Children and the GDPR Guidance (21 December 2017) at <https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf> at p. 19.

(*cont'd on next page*)

26 In Hong Kong, the Office of the Privacy Commissioner for Personal Data ("**PCPD**") has taken the view that "*children are identified as a vulnerable group who may have special needs in privacy protection*" (emphasis added).[13]

27 Against this backdrop, it is evident that minors' personal data would typically be of a more sensitive nature, especially when it concerns unique identifiers such as NRIC numbers. Accordingly, when it comes to the protection of "sensitive" personal data, organisations are required to take extra precautions and ensure higher standards of protection under the PDPA.

Whether the Organisation had complied with its obligations under section 11 of the PDPA

28 At the outset, during the investigation, the Organisation admitted that it had "*no idea of the PDPA*", and consequently, was not aware of its data protection obligations under Parts III to VI of the PDPA.

29 Notably, the Organisation's lack of awareness of its data protection obligations is not a legitimate defence to a breach under the PDPA, as set out in *Re M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 ("**M Stars Movers**") at [16]:

> "[i]t is a trite principle of law that ignorance of the law is no excuse. Thus, the Organisation's lack of awareness of its obligations under the PDPA cannot excuse its breach of the PDPA. The data protection provisions of the PDPA took effect on 2 July 2014 after a "sunrise" period of more than a year from 2 January 2013. Since then, organisations have had ample opportunities to develop and implement appropriate policies and practices to comply with the PDPA. In any event, an

13 Hong Kong, PCPD, 2015 Study Report on Online Collection of Children's Personal Data (December 2015) at <https://www.pcpd.org.hk/english/resources_centre/publications/surveys/files/sweep2015_e.pdf>.

> organisation's lack of awareness of its data protection obligations is not a legitimate defence to a breach."

30 Section 11(3) of the PDPA requires the Organisation to designate one or more individuals, i.e. the DPO, to be responsible for ensuring the Organisation's compliance with the PDPA.

31 The Organisation confirmed that there was "no person appointed for the role of Data Protection Officer".

32 By the Organisation's own admission, the Commissioner finds that the Organisation has failed to meet its obligations under section 11(3) of the PDPA. The Commissioner repeats the comments at paragraph 29 above that a lack of awareness of the obligations imposed by the PDPA does not amount to a legitimate defence against a breach by the Organisation.

33 The Commissioner takes this opportunity to reiterate the importance of the role of a DPO as set out in *M Stars Movers* at [33]:

> "[t]he DPO plays an important role in ensuring that the organisation fulfils its obligations under the PDPA. Recognition of the importance of data protection and the central role performed by a DPO has to come from the very top of an organisation and ought to be part of enterprise risk management frameworks…The DPO ought to be appointed from the ranks of senior management and be amply empowered to perform the tasks that are assigned to him/her… The DPO need not – and ought not – be the sole person responsible for data protection within the organisation…Every member of staff has a part to play…"

34 Generally, the responsibilities of a DPO include, but are not limited to:[14]

---

14 PDPC, Data Protection Officers at <https://www.pdpc.gov.sg/Organisations/Data-Protection-Officers>.

(a) ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data;

(b) fostering a data protection culture in an organisation and communicating personal data protection policies to stakeholders;

(c) handling and managing personal data protection related queries and complaints;

(d) alerting management to any risks that may arise with regard to personal data; and

(e) liasing with the Commission on data protection matters, if necessary.

35 From the foregoing, it is clear that the DPO plays a vital role in implementing and building a robust data protection framework to ensure an organisation's compliance with its obligations under the PDPA.

Whether the Organisation had complied with its obligations under section 12 of the PDPA

36 Section 12(a) of the PDPA requires an organisation to develop and implement policies and practices that are necessary to meet its obligations under the PDPA.

37 During the investigation, the Organisation confirmed that there was "*no personal data policy*" implemented and represented that the manner of handling the students' personal data was an "*unwritten SOP*".

38 By the Organisation's own admission, the Commissioner finds that the Organisation has failed to meet its obligations under section 12(a) of the PDPA.

Similar to the above, the Commissioner repeats his comments at paragraph 29 that a lack of awareness of the obligations imposed by the PDPA does not amount to a legitimate defence against a breach by the Organisation.

39 The Commissioner takes this opportunity to reiterate the role of data protection policies, as set out in *Re Aviva Ltd* [2017] SGPDPC 14 at [32]:

> *"*…[d]ata protection policies and practices developed and implemented by an organisation in accordance with its obligations under section 12 of the PDPA are generally meant to increase awareness and ensure accountability of the organisation's obligations under the PDPA…*"*

40 In addition, *M Stars Movers* highlights the importance of the need for organisations to develop and implement data protection policies and practices at [27] to [28]:

> "…[a]t the very basic level, an appropriate data protection policy should be drafted to ensure that it gives a clear understanding within the organisation of its obligations under the PDPA and sets general standards on the handling of personal data which staff are expected to adhere to. To meet these aims, the framers, in developing such policies, have to address their minds to the types of data the organisation handles which may constitute personal data; the manner in, and the purposes for, which it collects, uses and discloses personal data; the parties to, and the circumstances in, which it discloses personal data; and the data protection standards the organisation needs to adopt to meet its obligations under the PDPA.
>
> An overarching data protection policy will ensure a consistent minimum data protection standard across an organisation's business practices, procedures and activities..."

41 Finally, the Commissioner reiterates past observations on the benefits and importance of documenting an organisation's data protection policies and

practices in a written policy, as per *Re Furnituremart.sg* [2017] SGPDPC 7 at [14]:

> "[t]he lack of a written policy is a big drawback to the protection of personal data. Without having a policy in writing, employees and staff would not have a reference for the Organisation's policies and practices which they are to follow in order to protect personal data. Such policies and practices would be ineffective if passed on by word of mouth, and indeed, the Organisation may run the risk of the policies and practices being passed on incorrectly. Having a written policy is conducive to the conduct of internal training, which is a necessary component of an internal data protection programme."

42 It is clear from the foregoing that the development and implementation of written data protection policies and procedures are important in ensuring an organisation's compliance with its obligations under the PDPA.

Whether the Organisation had complied with its obligations under section 24 of the PDPA

43 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by implementing reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

44 The Commissioner's assessment of whether the Organisation had complied with its obligations under section 24 of the PDPA would be confined to the NRIC numbers of students. As admitted by the Organisation during the course of the investigation, the NRIC numbers of students were not supposed to be contained and disclosed in the PDF documents.

45 Whilst the encrypted Excel spreadsheet containing the students' personal data was provided by the MOE, the entire process of compiling the personal data into a separate Excel spreadsheet, converting the Excel

spreadsheet into PDF documents and uploading the PDF documents were actions that were conducted solely by the Organisation, without any external interference from the MOE or the entity responsible for maintaining the Organisation's website.

46 That said, the Organisation was unaware and unable to explain why the NRIC numbers were left in the minimised columns in the PDF documents.

47 In this regard, the Organisation's mistake of not realising that the NRIC numbers were present in minimised columns in the PDF documents and could have been disclosed without authorisation, could be quite easily repeated. Any person could simply copy the contents of the PDF documents and paste it on to another document, thereby resulting in further unauthorised disclosures of the students' personal data. Such potential impact and harm cannot be ignored, especially when it involves the NRIC numbers of 782 students who were also minors, and whose personal data would thus be considered to be more sensitive in nature.

48 It is precisely the fact that the unauthorised disclosure could have reoccurred quite easily due to the same mistake, that focus is drawn to the issue of whether the Organisation had complied with its obligations under section 24 of the PDPA.

49 On this issue, the Commission found that the Organisation did not appear to have taken sufficient steps towards protecting the personal data in its possession, to prevent the unauthorised disclosure of the personal data.

50 An example of an administrative security arrangement which the Organisation could have made in respect of the personal data in its possession,

was to "*[c]onduct regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data*".[15] The Organisation could have implemented staff training sessions to "*[e]nsure that staff are trained and familiar with the software used to process…documents containing personal data. For example, staff using spreadsheets should be aware of how sorting the data incorrectly may lead to errors*".[16] Similarly, the Organisation could have adopted any of the following measures to ensure that personnel using Microsoft Excel to process personal data were well apprised and updated on the functions of the software, in particular, the difference between columns that were "minimised" and "hidden" in an Excel spreadsheet:

(a) "*[e]nsure that new and existing staff receive regular training so that they are well apprised and updated on the proper procedures for processing and sending personal data*";[17]

(b) "*[train] staff to ensure only necessary personal data are extracted*";[18]

(c) "*[k]eep ICT security awareness training for employees updated and conduct such training regularly*";[19] and

---

15 Key Concepts Guidelines at [17.5].

16 PDPC, Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data (20 January 2017), at [2.1].

17 PDPC, Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data (20 January 2017), at [2.2].

18 PDPC, Guide to Data Protection Impact Assessment (1 November 2017), at [7.2].

19 PDPC, Guide to Securing Personal Data in Electronic Medium (revised on 20 January 2017), at [5.2].

(*cont'd on next page*)

(d) "*[provide] the appropriate training to ensure proper usage of the software used.*"[20]

51 Given the nature of the personal data in question, the Organisation had not taken into consideration what extra precautions would be required to protect the sensitive personal data of the students, who are minors.

52 The Key Concepts Guidelines express that an organisation should "*implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity*".[21] As set out in the Commission's Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data, "*[d]ocuments or communications that contain sensitive personal data should be processed…with* <u>*particular care*</u>" (emphasis added).[22]

53 The Key Concepts Guidelines goes on to state that (at [8.12]):

> "…given that there is generally greater sensitivity surrounding the treatment of minors, it may be prudent for organisations to consider putting in place relevant precautions, if they are (or expect to be) collecting, using or disclosing personal data about minors. For example, organisations that provide services targeted at minors could state terms and conditions in language that is readily understandable by minors, or use pictures and other visual aids to make such terms and conditions easier to understand. Other good practices could include placing additional safeguards against unauthorized disclosure of, or unauthorized access to, personal data of minors, or anonymising personal data of minors before disclosure, where feasible."

---

20 PDPC, Guide to Securing Personal Data in Electronic Medium (revised on 20 January 2017), at [17.7].

21 Key Concepts Guidelines at [17.3].

22 PDPC, Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data (20 January 2017), at [2.2].

(*cont'd on next page*)

54 In this regard, the Commissioner agrees with the OPC that, in the context of children's personal data, safeguards that are implemented must be "*commensurate with the amount and potential sensitivity of the information at risk"* and if the appropriate safeguards are not implemented, this "*could, in the wrong hands, put children at unnecessary risk of harm*".[23] In that case, the OPC found that the personal data of approximately 316,000 Canadian children, in addition to approximately 237,000 Canadian adults, that were in the possession of a toy manufacturer had been compromised as the organisational and technological safeguards that were implemented at the time of the data breach incident were not commensurate with the amount and potential sensitivity of the personal data.

55 When it comes to the protection of "sensitive" personal data, the Organisation had failed to take extra precautions to guard against and prevent unauthorised disclosures of personal data, and failed to ensure a relatively higher standard of protection of personal data under the PDPA. At a minimum, the Organisation ought to have ensured that its staff in charge of creating, processing and converting the Excel spreadsheets were given proper and regular training to equip them with the knowledge to utilise the correct function to convert the Excel spreadsheets into PDF documents that were routinely published on the Organisation's website.

56 Not only did the Organisation fail to develop and implement the appropriate security arrangements upon the PDPA coming into full force on 2 July 2014, this failure had carried on well after 2 July 2014. Considering how

---

23 *PIPEDA Report of Findings #2018-001: Connected toy manufacturer improves safeguards to adequately protect children's information* (8 January 2018) at <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-001/> at Overview.

there were two other instances where the Organisation had uploaded the personal data of students in the same manner, specifically for the 2015 and 2016 Championships, the Organisation's prolonged failure to develop and implement reasonable security measures (for instance, in the form of proper and regular staff training to equip staff with the knowledge to use the right Microsoft Excel feature) to protect the personal data is also taken into consideration in this decision.

57 Given the absence of any security arrangements to protect personal data in its possession against unauthorised disclosure, the Commissioner finds that the Organisation has contravened section 24 of the PDPA.

Directions

58 Having found that the Organisation is in breach of sections 11, 12 and 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

59 In assessing the breach and determining the directions to be imposed on the Organisation, the Commissioner took into account, as a mitigating factor, the Organisation's prompt remedial actions to rectify and prevent the recurrence of the data breach.

60 The Commissioner also took into account the following aggravating factors:

(a) the personal data disclosed involved the NRIC numbers of minors, which constitute personal data of a sensitive nature, and the

disclosure of which could cause substantial actual or potential harm to the students;

(b) the Organisation showed a lack of awareness of its obligations under the PDPA; and

(c) the Organisation caused quite some delays in the investigation process. Despite the approval of an extension of time for responding to the Commission's Notice to Require Production of Documents and Information issued under the Ninth Schedule of the PDPA, the Organisation only responded after the Commission had sent subsequent reminders requesting for the Organisation's response, and only after the President of the Organisation was copied in one of such email reminders.

61 The Commissioner has also reviewed the representations made by the Organisation seeking a reduction in the financial penalty imposed, a summary of which follows:

(a) The Organisation is a small registered charity with a thin budget;

(b) The Organisation did not appoint a Data Protection Officer and as such were unaware of the requirement to have a Data Protection Policy;

(c) The Organisation took immediate remedial action;

(d) The breach was due to inadvertence and ignorance that the NRIC data could be seen on its website;

(e) The Organisation acknowledged the unauthorized disclosure of 782 students but that there is no specific information to suggest that the

data of the students involved in the 2015 and 2016 tournaments had been similarly disclosed;

(f) The delay was caused by their surprise at the lapse and their need to obtain external advise as well as the Organisation's internal approval process to respond to the PDPC;

62 It should be noted that the Commissioner had already taken (c) above into consideration in determining the financial penalty quantum. The Commissioner finds that the rest of the above representations do not justify a reduction in the financial penalty. The PDPA applies to all organisations and the mere fact that the Organisation is a small charity is not a mitigating factor. If the Organisation has cash flow issues, it is open to the Organisation to request that the penalty be paid in installments. Also, inadvertence and ignorance of the law are not mitigating factors.

63 On the point of delay, the Organisation took 2 months to respond to the first Notice to Produce issued to the Organisation. The initial deadline to respond to the Notice to Produce was on 23 June 2017, 2 weeks after the Notice to Produce was issued. PDPC granted the Organisation's request for an extension of time to respond to the Notice to Produce by 31 July 2017. The Organisation failed to meet this extended deadline and did not respond even after a first reminder was sent on 2 August 2017. The Organisation only responded to the Notice to Produce after a second reminder was issued on 10 August 2017 and copied to the President of the Organisation. The Organisation had already been granted the requested 5-month extension of time to respond and failed to do so within that time, only responding after 2 reminders were issued. The Commissioner finds that the 7 weeks given to the Organisation to respond was more than sufficient to engage third party experts to assist the

Organisation in its investigations and to obtain the necessary internal approval. The delay was therefore unacceptable.

64 In consideration of the relevant facts and circumstances of the present case, the Commissioner hereby directs the Organisation to:

(a) pay a financial penalty of S$30,000 within 30 days from the date of this direction, failing which interest, at the rate specified in the Rules of Court in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty;

(b) appoint a DPO within 30 days from the date of this direction;

(c) develop and implement policies and practices that are necessary for the Organisation to meet its obligations under the PDPA within 30 days from the date of this direction; and

(d) inform the Commission of the completion of each of the above directions in (b) and (c) within 1 week of implementation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION