# Club the Chambers

## [2018] SGPDPC 24

Tan Kiat How, Commissioner — Case No DP-1701-B0439

Data Protection – Protection obligation – Context of disclosure rendered personal data sensitive – Stronger controls needed to protect sensitive personal data

4 October 2018.

### Background

1 The Organisation had displayed A4-size notices comprising of photocopies of the identity documents of 11 individuals whom the Organisation had banned from entry, along with descriptions of why those individuals had been banned. It is clearly well within the prerogative of an organisation to ban individuals from entry into its premises as a consequence of flouting its rules, in particular where the actions of such individuals affects the organisation's ability to maintain order and prevent criminal and other undesirable activities from being carried out. The question with which the Commissioner is concerned is whether the flouting of rules by individuals provides an organisation with carte blanche to treat the personal data of those individuals in any manner it sees fit. The Commissioner's findings and grounds of decision are set out below.

**Material Facts**

2 The Organisation operates several gaming centres, or clubs, where members use computers connected by a Local Area Network ("**LAN**") to play multi-player games. The LAN gaming centre in question was the Organisation's Hougang branch (the "**LAN shop**").

3 To play at the LAN Shop, an individual must first sign up to become a member. All members are subject to the Organisation's rules and regulations. These rules stipulate that members who engage in prohibited behaviour, e.g. online gambling, viewing of pornography, theft and truancy, will be banned from entry. According to the Organisation, the rationale for banning members is to maintain order and to prevent criminal and other undesirable activities from being carried out on the Organisation's premises.

4 On 11 January 2017, the Personal Data Protection Commission ("**PDPC**"), acting on a tip-off published in an online news report[1], inspected the LAN Shop and found that the Organisation had posted notices ("**Notices**"), comprising enlarged photocopies of the identity documents (e.g. student pass, employment pass, Singapore Armed Forces identity card) of 11 individuals whom the Organisation had banned from entry into its premises. Each Notice contained personal data of a member who was banned.

5 The Notices disclosed different types of personal data, including a member's name, photograph, NRIC number/FIN, student identification

---

1 The Mothership, "Gaming shop resorts to shaming misbehaving kids, but giving away too much personal info" (30 December 2016) <http://mothership.sg/2016/12/gaming-shop-resorts-to-shaming-misbehaving-kids-but-giving-away-too-much-personal-info/>.

number, mobile phone number, and name of employer, occupation, and remarks about a member ("**remarks**"). The Organisation provided these remarks to explain why the members had been banned from the LAN Shop, which included the following:

(a) "*Banned for skipping classes and being very rude to his parents*";

(b) "*Banned for surfing pornography*";

(c) "*Banned for using others' Ezlink card*";

(d) "*Banned for stealing money and captured by CCTV*";

(e) "*Caught for stealing iPhone*"; and

(f) "*Caught online gambling during routine checks by police and arrested inside the centre*".

6 The personal data in question, except for the remarks, had been collected at the time of application when the individuals filled up membership forms. The Organisation's stated intention for displaying the Notices is for the purpose of helping its staff to identify members who had been banned from the LAN Shop. The staff will deny entry to the LAN Shop to banned members.

7 The sole proprietor of the Organisation alleged that he had instructed his staff to remove the Notices prior to 2 July 2014 when the data protection provisions of the Personal Data Protection Act 2012 ("**PDPA**") came into effect. However, the Notices continued to be displayed in the LAN Shop until they were finally taken down sometime between 11 January 2017 to 26 January 2017.

8 At the material time, the Organisation did not have in place any personal data protection policies or internal guidelines, although it claimed it had appointed a data protection officer.

## Findings and Basis for Determination

### *Two Issues for Determination*

9 The relevant issues for determination in this case are:

(a) *whether the Organisation obtained consent from its customers to disclose the personal data found in the Notices pursuant to section 13 of the PDPA;*

(b) whether the disclosure of personal data was for a purpose that a reasonable person would consider appropriate in the circumstances pursuant to section 18(a) of the PDPA; and

(c) whether the Organisation developed and implemented the necessary data protection policies and practices pursuant to section 12(a) of the PDPA.

### *Whether the Organisation obtained consent from its customers to disclose the personal data found in the Notices*

10 The Commissioner finds that the Organisation failed to obtain consent from its customers who were the subject of the Notices. The Commissioner's explanation of this finding is set out in greater detail below at paragraphs 17 to 21 in discussing the Organisation's section 18(a) obligations.

***Whether the disclosure of personal data of its members was for a purpose that a reasonable person would consider appropriate in the circumstances pursuant to section 18(a) of the PDPA***

11 Pursuant to section 18(a) of the PDPA, 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. Where the purpose of collection, use or disclosure does not fall within one of the excepted general purposes set forth in Schedules Two, Three and Four, the purpose has to be both appropriate and also notified to the individual. Where the general purpose of collection, use or disclosure falls within one of the aforementioned exceptions, the specific purpose must still be reasonably appropriate, although there is no need to notify the individual subject to section 20(4) of the PDPA.

12 As a preliminary point, it was not disputed that the data contained in the Notices, which included details such as the banned member's name, photograph, NRIC number/FIN, student identification number, name of employer and occupation, fell within the definition of "personal data" under section 2(1) of the PDPA as it was possible to identity the 11 banned members from such details when taken as a whole. Also, given that the reason for the ban set out in each of the Notices was stated below the copy of the NRIC of each banned member, these reasons would also constitute personal data of the member. It was also not disputed that the personal data of the banned members was in the Organisation's possession and under its control at the material time.

13 Based on the investigations, the Commissioner finds that the purpose of disclosure of the 11 banned members' personal data was for an inappropriate purpose that breaches section 18(a) of the PDPA. The reasons for this finding are set out below.

*The Purpose of the Notices was to assist staff in identifying banned members and to inform banned members that they were prohibited entry into the LAN Shop*

14 The sole-proprietor of the Organisation in his statement, made clear that the purpose for the display of the Notices was to assist staff in identifying banned members and to inform banned members that they were prohibited entry into the LAN Shop and the reason(s) for the ban.

15 In answer to the question "[p]lease state the purpose of the collection, use and disclosure of the personal data of those individuals", the sole-proprietor stated, *inter alia*, that:

> "The purpose of collection, use and disclosure was to facilitate the application of membership and the provision of LAN gaming services to members which includes maintaining the rules and regulations.
>
> The rules and regulations such as banning members from entry due to surfing porn, online gambling or skipping schools (*sic*) is necessary to maintain order and prevent criminal activities from occurring in our premises. In fact, the aforesaid was encouraged by undercover police officers when they arrested people for online gambling.
>
> **Accordingly, we put the Notices to inform our staff and also those members banned from our clubs that they are prohibited entry**. Members never challenged or demanded us to bring down the Notices, but asked us for reasons. For example, a student will be informed that he has been banned because he skipped school. In this regard, some parents who complain to us for allowing their children to play in the LAN gaming shop will give permission for us to put the personal data of their children up to shame them so they will not do it again, but other parents will refuse.
>
> As for adults, some will ask us why we put up the Notices, and we will inform them that they have been caught by the police for online gambling.
>
> The students and adults need to show to us why we should remove the ban and Notices. For example, a student needs to show us good results. Likewise, the adult needs to show us that he did not commit the offence like surfing porn or online gambling, or only given a warning by the police.

> At the end of the day, CTC did not disclose the personal data with ill intent but rather to adhere to the laws and ensure our members comply with the laws as well. That said, **I admitted that we did post the Notices up and there were better ways to inform our employees and members of the ban**. (emphasis added)[2]

16 From the above, it appears that the Organisation encountered situations where members were potentially using their premises for criminal activities such as online gambling or were playing truant and were in the LAN Shop when they were meant to be in school. To manage this, the Organisation decided to ban members who were suspected of committing an offence or undertaking any undesirable activities in their premises or playing truant. The purpose of the Notices was to inform the Organisation's staff which members were banned and to inform banned members of their ban and the reasons for the ban. Whilst the intentions are laudable, the modality of execution fell short.

17 At this juncture, the Commissioner would like to deal with the Organisation's claim that *"some parents … will give permission for us to put the personal data of their children up…"*. The first point to take note of here is that the Organisation does not claim that consent was obtained from all its members who were the subject of Notices which were displayed. In fact, this is an admission that consent to display the Notices was not obtained from all of the members who were the subject of Notices. Even with respect to the claims made that consent was obtained in some of the cases, the Organisation failed to adduce any evidence of having obtained any such consent to support this claim other than the bare assertion made by the sole-proprietor of the Organisation.

---

[2] Witness Statement dated 3 February 2017.

18 *The other point that the Commissioner would like to deal with as a preliminary issue is the claim that "[m]embers never challenged or demanded us to bring down the Notices."*. It should be noted that the failure to challenge or demand that the Notices be removed does not indicate that the member has unequivocally consented to the display of the Notices. The Organisation is required to either specifically obtain consent from the member to display the Notice or rely on deemed consent. The facts of this case, as uncovered during the investigations, does not lend itself to a finding that members are deemed to have consented to the display of the Notices.

19 In this regard, given that the purpose of the Notices was limited to assisting staff in identifying banned members and to inform banned members that they were prohibited entry into the LAN Shop and the reason(s) for the ban, a reasonable person would not consider it appropriate to display the Notices to everyone that enters the LAN Shop. In fact, even the sole-proprietor of the Organisation admits that other better ways existed to inform staff and banned members of the ban. Clearly, a simple way of doing so would have been to maintain an internal black list that only the staff on duty would be able to consult.

20 Given the above, it is telling that the sole-proprietor instructed his staff to remove all the Notices before the PDPA came into effect. In this regard, the sole proprietor in his witness statement, in answer to the question "[p]lease state whether CTC (ie the Organisation) had taken any measures as of 30 December 2016 to prevent its employees to (*sic*) collect, use and disclose personal data without consent and notification. If so, please provide details of the measures taken", stated that:

> "I actually instructed my employees to take down those the (sic) Notices before the Personal Data Protection Act came into effect.

> But I do not visit the clubs (including the LAN Gaming Shop) regularly so I was not able to monitor whether they did in fact take down the Notices.
>
> However, they took down the Notices before I received your notice to produce but I could (sic) not remember the date. They took it down during the Chinese new Year."

21 In the final analysis, the Organisation's intention to withhold its services from certain categories of users cannot be faulted nor should personal data protection laws impede such intentions. However, the manner in which it had carried out this purpose left much to be desired. The use of personal data to maintain an internal black list of customers that are banned from the cybercafe is an appropriate purpose. Section 18 of the PDPA requires that such use be notified, and this could easily have been achieved with clear notification that some of the personal information provided by customers of the cybercafe during registration may be used for the purpose of managing the ongoing customer relationship, including the provision or suspension of services due to the customer's breach of the Organisation's rules. This would be an eminently appropriate purpose and, once notified, there would have been consent if the customer continues to make use of the cybercafe's facilities and services. One further point to highlight is that not all personal data disclosed in the Notices is required to achieve this purpose; photocopies of NRIC and FIN cards in particular need not have been used to achieve the stated purpose.

22 The manner of disclosure also left much to be desired. As the owner of the Organisation well knows, the black list need not be publicly displayed but can be kept as an internal list. The placement of the Notices also detracts from the stated purpose of assisting staff in the identification of persona non grata. These Notices were placed on the wall behind the counter such that when a member of staff is engaging with a customer, the Notices will be behind him.

This detracts from its effectiveness as a black list for staff, but suggests that it was intended to name and shame customers.

***Whether the Organisation developed and implemented the necessary data protection policies and practices pursuant to section 12(a) of the PDPA***

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

24 In the present case, the Organisation admitted to the PDPC that, at the material time, it did not have in place any personal data protection policies or practices, or even internal guidelines with respect to personal data. As such, the Organisation was in breach of section 12(a) of the PDPA.

**The Commissioner's Directions**

25 Given the Commissioner's findings that the Organisation is in breach of its obligations under sections 13, or in the alternative section 18, and 12(a) of the PDPA, the Commissioner is empowered under section 29 of the PDPA to issue the Organisation such directions as it deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million.

26 In assessing the breach and determining the directions to be made, the Commissioner took into account, as an aggravating factor, the actual or potential harm that was posed to the 11 banned members due to the sensitive nature of the personal data disclosed.

27 The Commissioner also took into account the following mitigating factors:

(a) the Organisation was cooperative during investigations and the sole director of the Organisation delayed his overseas business trip in order to give his witness statement to the PDPC;

(b) the Organisation did not have malicious intentions in disclosing the personal data and had only displayed the Notices to maintain order in the LAN Shop and discourage criminal and undesirable activities from being carried out on its premises; and

(c) the Organisation took prompt remedial action to remove the Notices before the PDPC sent it a Notice to Produce Documents and Information.

28 Having carefully considered all the relevant factors noted above, pursuant to section 29(2) of the PDPA, the Commissioner hereby directs that the Organisation to:

(a) comply with section 12(a) of the PDPA by developing and implementing policies and practices that are necessary for the Organisation to meet the data protection provisions of the PDPA within 60 days of the date of the Commissioner's direction; and

(b) The Organisation pay a financial penalty of S$7,000 in accordance with the Commissioner's direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

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

---