

This decision is subject to final editorial corrections approved by the Commission and/or redaction pursuant to the publisher's duty in compliance with the law, for publication in LawNet.

**The Management Corporation Strata Title Plan No. 3696
Eagle Eye Security Management Services Pte Ltd**

[2017] SGPDPC 11

Personal Data Protection Commission — Case No DP-1610-B0275

Data Protection – Protection obligation – Access to personal data –
Insufficient physical and administrative security arrangements

Data Protection – Data intermediary – Obligations of organisation and data
intermediary

29 June 2017.

Introduction

1 Sometime in December 2015, the Personal Data Protection Commission (the “Commission”) had investigated into a complaint in relation to the failure by a security company to safeguard the visitor logbook of Prive Executive Condominium (the “Condominium”), which contained personal data of the visitors. The security company was found in breach of Section 24 of the Personal Data Protection Act 2012 (“PDPA”) for leaving the logbook unattended and failing to protect the logbook from prying eyes. The case is published as *Spear Security Force Pte. Ltd.* [2016] SGPDPC 12.

2 A similar breach has again taken place at this Condominium. This time round, the breach took place under another security company, the 2nd Respondent (“Eagle Eye”), which was engaged by the 1st Respondent (“MCST

3696”), the Management Corporation Strata Title (“MCST”) of the Condominium, for its security services.

3 Following a complaint made to the Commission, the Commission proceeded to investigate into the matter. The Commission found both the 1st and 2nd Respondents in breach of their respective obligations under Section 24 of the PDPA. The Commission now sets out its grounds of decision of the matter.

Material Facts

4 The data breach incident took place in the evening of 16 October 2016. The Complainant had observed that a logbook that was placed on a table next to the gantry into the Condominium was left unattended. The Complainant subsequently took photographs to show that the logbook was left open on the table and unattended by the security guards. These photographs were sent to the Commission for its investigation.

5 The gantry was about 30 to 50 metres away from the guardhouse, and led directly to the swimming pool of the Condominium. The logbook was used to record the attendance and details of the coaches who conduct swimming lessons at the Condominium. The logbook would therefore contain the dates and times of entry into the Condominium and the NRIC numbers of the coaches.

6 Based on the Commission’s investigation, the Commission found that there was no security guard attending to the logbook from the hours of 8 pm to 10.30 pm. There was supposed to be a night-shift security guard to be stationed at the table where the logbook was located. However, the night-shift guard had reported that he was ill that evening, and his replacement had only arrived for duty at 10.30 pm. Accordingly, the only security guards that were in the vicinity

from 8 pm to 10.30 pm were the security guards that were stationed at the guardhouse, away from the gantry.

7 Although the security guards were stationed at the guardhouse, Eagle Eye claimed that they were within close proximity of the logbook, and keeping an eye whilst in the guardhouse.

8 The MCST 3696 and Eagle Eye also claimed that the security guards had previously been specifically instructed to close the logbook when not in use and to keep the book in the guardhouse if no security guard was stationed at the table. Additionally, they claimed that these security guards were reminded to exercise due care and diligence to safeguard personal data; were advised on the PDPA; and warned about severity of penalty for disclosure of personal data.

9 Following the data breach incident, the MCST 3696 and Eagle eye had removed the table at the Condominium gantry so that all visitor registrations would only be done at the guardhouse. This was to ensure that the logbook was kept in the guardhouse at all times.

Commission Findings

10 The information that was contained in the logbook, namely, the NRIC number and the dates and times of the entry and departure from the Condominium, would constitute “personal data” under Section 2 of the PDPA of the coaches who came to the Condominium. The information allows for the identification of the individual, and the date and timings in which the individual had entered and left the premises. In particular, the NRIC numbers of the coaches are generally considered to be of a sensitive nature, as it is widely used

for business purposes and transactions with the government,¹ and could be used to cause harm should such information fall into the wrong hands.

11 Accordingly, since the logbook contains personal data of the individual coaches, it must be protected under Section 24 of the PDPA.

12 The issues that arise from this case are as follow:

- (a) What was the relationship between MCST 3696 and Eagle, and what were their respective obligations under the PDPA;
- (b) Whether MCST 3696 and Eagle Eye complied with their respective obligations under the PDPA.

Relationship between MCST 3696 and Eagle Eye and their respective obligations

13 The MCST 3696 had engaged Eagle Eye to provide security guard services pursuant to an agreement on 15 August 2016.

14 As part of the security services, Eagle Eye was to record the movement of persons entering or leaving the premises of the Condominium. This included the maintaining a logbook of coaches who were entering or leaving the premises of the Condominium.

15 The recording and safekeeping of the logbook were activities that fall under the definition of “processing” of personal data under Section 2(1) of the PDPA. Given that MCST 3696 had engaged Eagle Eye to carry out such services (as part of the overall security services), Eagle Eye was a data

¹ Advisory Guidelines on NRIC numbers.

intermediary to MCST 3696 (the organisation) in relation to the handling and safekeeping of the logbook.

16 As an organisation, MCST 3696 has the primary role and duty to protect personal data in its possession or control under Section 24 of the PDPA. The organisation held the primary role and duty to protect personal data, even though it had engaged a data intermediary to protect the personal data as well. This principle has been elucidated in the case of *The Cellar Door Pte Ltd and Global Interactive Works Pte. Ltd.* [2016] SGPDPDC 22. As for Eagle Eye, although it has fewer obligations to meet under the PDPA (pursuant to section 4(2) of the PDPA), it still needs to protect personal data in its possession under Section 24 of the PDPA.

17 We now turn to examine whether MCST 3696 and Eagle Eye have complied with their respective obligations to protect the logbook under Section 24 of the PDPA.

Whether MCST 3696 and Eagle Eye have complied with their respective obligations to protect personal data under Section 24 of the PDPA

18 In relation to Eagle Eye, the Commission has found Eagle Eye to be in breach of its obligations under Section 24 of the PDPA.

19 First, whilst Eagle Eye claims that it had informed the security guard to keep the logbook closed when not in use and to keep the book in the guardhouse if no security guard was stationed at the table, the instructions were clearly ineffective, as none of the security guards had carried out those instructions. As the Complainant had found on 16 October 2016, the logbook was left unattended and open on the table. Further, the instructions themselves were bare and incomplete, as they do not, for example, inform the security guards how to

organise themselves to ensure that the logbook is closed at all times when not in use, or who was responsible to carry out the task. The failure by Eagle Eye to provide proper instructions to its security guards was a dereliction of its duty to ensure that there were reasonable security arrangements to protect the personal data in the logbook.

20 Moreover, it was not enough for the organisation to simply provide instructions to the security guards to safekeep the logbook without doing more – ie putting in place actual processes or practices to protect the logbook. Without having actual processes or practices in place to protect personal data, Eagle Eye’s instructions were but empty instructions with little effect. This can be seen in the manner in which the security of the logbook appears to have been carried: on an ad-hoc basis, where there is no coordinated and comprehensive effort to ensure that the logbook was safeguard or safekept with the security guards at all times. And indeed, this has been laid bare by the Complainant being able to take photographs of the logbook without the security guards noticing.

21 Additionally, the alleged instructions were not documented. This makes it hard to disseminate the message to all the security guards, especially to the new employees joining the organisation. As discussed in in *Furnituremart.sg* [2017] SGPDP 7, without having written policies or practices, it would be difficult to promulgate the policies or practices effectively to the employees and staff of the organisation.

22 Second, while Eagle Eye had a data protection policy in place, the policy was spartan in terms of the policies that govern the protection of the logbook. The only reference to the protection of personal data was a line which mentioned:

“To ensure that personal rights to confidentiality are respected in compliance with the Personal Data Protection Act 2012 and no disclosure of personal data of resident, visitor, contractor, vendor, delivery and etc”.

The policy does not elaborate further on how these may be translated into actual practices or processes to protect the logbook. As mentioned in *Tiger Airways Singapore Pte Ltd, SATS Ltd and Asia-Pacific Star Limited* [2017] SGPDP 6, it is important for an organisation to ensure that its policies are contextualised to its operations, so that they are pertinent and relevant to the organisation’s work or operations on the ground, and meaningful and useful to employees in the context of their work or responsibilities. A simple or bare statement in a policy telling employees to comply with the PDPA (for example) would not actually inform them how to protect personal data in the context of what they are doing.

23 Third, Eagle Eye did not seem to have a contingency plan for the safekeeping of the logbook when the security guard fell sick and had to be replaced by another security guard. When the replacement guard came late, that had apparently led to the shortage of a security guard to be stationed at the table to look after the logbook. Rather than returning the logbook to the guardhouse, the logbook was simply left on the table unattended. In the Commission’s view, there ought to have been some form of system or process to ensure that when the security guards are unavailable to be stationed at the table, the logbook would, by default, be returned back to the guardhouse for safekeeping. Again, this accentuates the point that there was no system in place to ensure the proper safekeeping of the logbook.

24 Eagle Eye claimed that their security guards were in close proximity of the logbook, since they were stationed at the guardhouse, and had kept an eye on the logbook. However, this was not the same as safeguarding the logbook

itself. The fact the Complainant was easily able to take photographs of the contents of the logbook and the surroundings, without any of the security guards noticing, is testament to the need for having close supervision of the logbook, which may only be achieved in this case by keeping the logbook with the security guards. By being stationed at the guardhouse, this made supervision and monitoring of the logbook difficult, and increases the risk of the security guards being blind-sided to any unauthorised access of the logbook that was left at the table. The difficulty of supervision and monitoring was exacerbated by the fact that the security guards' attention would have been diverted (at times) to the activities at the guardhouse, and away from the logbook.

25 With regards to MCST 3696, it had the primary and shared responsibility with Eagle Eye to protect personal data.

26 The need to meet this primary responsibility ought to have been drawn into sharp focus for MCST 3696, as this was not the first time that the hired security guards of the Condominium had left the logbook unattended. As mentioned above, the Commission had found the previous security guard company to be in breach of PDPA for a similar incident, and had been issued a warning for it. Given that the previous security company was issued such a warning, the MCST 3696 ought to have exercised closer supervision over the implementation and adoption of the policies and practices to protect the personal data collected by the Condominium. For example, by engaging with Eagle Eye in the planning and development of policies and practices that would be appropriate in the Condominium's setting to protect personal data, or by having general oversight over the security of the personal data. After all, having gone through the previous experience of the data breach incident, there would have been lessons learnt and improvements to be made, which the MCST 3696 can impart or share with the incoming security guard company, Eagle Eye, for

developing its policies and practices to protect personal data at the Condominium.

27 However, the MCST 3696 had failed to meet this primary responsibility to protect personal data. As mentioned above, the Commission has found a lack of adequate policies and processes that were in place to protect personal data. This is evident, given there was only one line in Eagle Eye's policy on personal data protection. Next, it was already established above that there was no system in place at the Condominium for the safekeeping of the logbook at all times – and indeed, the logbook was found to be left open on the table in this case. Additionally, from the responses provided to the Commission, it would appear that the only thing that the MCST 3696 did was to remind the security guards at the meeting to secure the logbook, which fell far short of providing that supervision and oversight (described above) for the protection of personal data.

28 Given the MCST 3696's failure to provide that supervision and oversight to ensure the security of the personal data in the logbook, the Commission has found the MCST 3696 to also be in breach of Section 24 of the PDPA.

Actions taken by the Commission

29 For the reasons above, the Commission has found that both Eagle Eye and MCST 3696 are in breach of their respective obligations under Section 24 of the PDPA. In this regard the Commission is empowered under Section 29 of the PDPA to give Eagle Eye and MCST 3696 such directions as it deems fit to ensure compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding \$1 million as the Commission thinks fit.

30 However, in view that Eagle Eye and MCST 3696 have taken reasonably adequate steps to remedy the lapses, as set out above at paragraph 10, during the course of the investigations, the Commission has decided not to impose any directions against them. Instead, it has decided to issue a Warning against Eagle Eye and MCST 3696 for the breach of their respective obligations under Section 24 of the PDPA.

31 The Commission emphasises that it takes a very serious view of any instance of non-compliance with the PDPA, and it urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.
