

CASE UPDATE



CASE UPDATES OF ENFORCEMENT ACTIVITY BY THE SINGAPORE PERSONAL DATA PROTECTION COMMISSION

24 July 2017

Introduction

1. The Personal Data Protection Commission (“**PDPC**”) has issued three recent decisions which should be of great interest to property owners, management corporations (“**MCSTs**”), council members, managing agents, service providers and subsidiary proprietors. In this case update, we summarise the three cases, and analyse their significance to your business.

For any queries relating to this article, please contact:

Tan Tee Jim S.C.
tanteejim@leenlee.com.sg

Zechariah J. H. Chan
zechchan@leenlee.com.sg

Case Study 1: No Breach of Consent and Notification Obligations by MCST and Managing Agents of Condominiums

2. On 12 June 2017, a joint decision was issued for three separate cases involving MCSTs and condominium managing agents (the “**Complainees**”). These cases all involved the disclosures of documents (voting lists and minutes of meetings) containing personal data on condominium noticeboards. The personal data comprised residents’ names, addresses, and in one of the cases, the residents’ voting shares. The PDPC found that there was no breach of the Consent and Notification Obligations (these Obligations are explained below) in the three cases.

Authors:
Tan Tee Jim S.C.
Zechariah J. H. Chan
Tan Sih Im
Basil Lee

Lee & Lee
50 Raffles Place, #06-00
Singapore Land Tower,
Singapore 048623
T : (65) 6220 0666

3. Under the Personal Data Protection Act (“**PDPA**”), organisations must obtain the consent of an individual for the collection, use or disclosure of his personal data (the “**Consent Obligation**”). Organisations must also notify an individual of the purposes for which they intend to collect, use or disclose his personal data before they actually collect, use or disclose the personal data (the “**Notification Obligation**”).

For more legal updates, please visit the News & Publication Section of Lee & Lee’s website at www.leenlee.com.sg.

4. In reaching its decision, the PDPC considered three main issues:
 - First, whether the Complainees could rely on any exceptions under the PDPA;
 - Second, whether the Complainees had disclosed more personal data than was permissible; and
 - Third, in two of the cases, whether the Complainees had disclosed personal data for longer than was permissible.

Disclaimer: The copyright in this document is owned by Lee & Lee. No part of this document may be reproduced without our prior written permission. The information in this update does not constitute legal advice and should not form the basis of your decision as to any course of action.

5. On the first issue, the PDPC held that while the Complainees had not obtained consent nor notified residents of the disclosure of their personal data, they were able to rely on two exceptions under the PDPA. The first exception is that organisations may disclose personal data without obtaining consent or giving notification if required or authorized under the PDPA or any other written law. In this case, the Building Maintenance and Strata Management Act (“**BMSMA**”) required management corporations to display a list of the names of voters entitled to vote at the general meeting on the notice board maintained on the common property.

6. Similarly, management corporations had to display a copy of minutes of meetings of the council or executive committee on the notice board. While the BMSMA had not expressly stipulated the information that ought to be included or omitted in the minutes, the PDPC was of the view that it was reasonable for the names and addresses of the voters to be included. The names would reasonably form a part of the minutes in order to identify and record the persons in attendance. The addresses would in turn establish the basis for the attendee's attendance, establishing him as a subsidiary proprietor or a subsidiary proprietor's representative.
7. The second exception is the "public availability" exception. Essentially, if any member of the public could obtain or access the data with few or no restrictions, then the data would be publicly available and would not be subject to the Consent and Notification Obligations. In this case, because all the personal data concerned (the names, addresses and voting shares of the residents) were accessible from the property's strata roll, and there are few restrictions for a member of the public to gain access to the strata roll, the personal data were considered publicly available.
8. In addition, there are few restrictions on a member of the public purchasing such information from the Singapore Land Authority. The PDPC noted that anyone can purchase property title information, property ownership information and land information, which include name, unit number and share value of the lot, for a prescribed fee. Similar to the strata roll, SLA imposes no or few restrictions on the purchase.
9. As regards the second issue, the PDPC found that the Complainees had *not* disclosed more personal data than was permissible because the personal data disclosed was relevant to the agenda of the meeting (in the case of the disclosure of the residents' names and unit numbers in the minutes of meeting), and was in any event publicly available information.
10. On the third issue, the PDPC found that keeping the voter list on the notice board for up to two months after the council meeting was *not* unnecessarily long. However, the PDPC cautioned that, notwithstanding the application of any exceptions under the PDPA, the disclosure of irrelevant personal data or disclosure of personal data for unnecessarily long periods might attract sanctions.
11. This case provides much needed guidance to the many MCSTs in Singapore and their managing agents as they balance the requirements of running an estate and at the same time, staying compliant with the PDPA. MCSTs and their managing agents should be careful to ensure that disclosures are relevant to the purposes, are not made for unnecessarily long periods and are reasonable in their circumstances.

Case Study 2: Breach of Protection Obligation by Eagle Eye Security Management Services

12. On 29 June 2017, the PDPC issued a warning to Eagle Eye Security Management Services ("**Eagle Eye**") and the MCST of Prive EC for failing to put in place reasonable security arrangements to prevent unauthorised access to a visitor logbook containing personal data. In this case, a visitor logbook which contained dates and times of entries into a condominium by swimming coaches and the swimming coaches' NRIC numbers were left unattended on a table next to a gantry into the condominium. The logbook had been left unattended for 2.5 hours.
13. The PDPC found that both Eagle Eye and the MCST had breached the Protection Obligation, which obliges organisations to protect personal data in their possession or control. Eagle Eye had failed to provide proper instructions to its security officers to ensure that the logbook was properly kept.

Further, Eagle Eye did not have processes or practices in place to protect personal data, and its data protection policy was spartan and failed to give any meaningful or useful guidance to its employees. In fact, Eagle Eye's data protection policy merely stated:

"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".

14. The PDPC also found the MCST to be in breach of its Protection Obligation. Even though it had engaged Eagle Eye as its data intermediary to protect personal data, it continued to be primarily responsible for the protection of personal data. In this regard, it had failed in its obligation. It had not exercised close supervision and oversight over the adoption of policies and practices to protect the personal data it collected, despite the fact that it had previously been found by the PDPC to have breached its Protection Obligation due to security guards (from another security company) leaving the logbook unattended.
15. As a result of the breaches, Eagle Eye and the MCST were issued with a warning by the PDPC. In coming to this decision, the PDPC placed emphasis on the measures taken by Eagle Eye and the MCST to remedy the lapses, by shifting all visitor registrations to the guardhouse and ensuring the logbook was attended to at all times.
16. This decision carries a few important lessons:
 - (a) First, it is important to provide proper and meaningful instructions which are properly contextualized to employees to help them understand the measures that they must take to protect personal data. These instructions should be written, and should provide for contingencies.
 - (b) Second, the engagement of a data intermediary to deal with personal data does not discharge an organisation's obligations over the personal data. An organisation must continue to exercise proper supervision and oversight to ensure that personal data remain properly protected.
 - (c) Third, if a data breach is discovered, an organisation should take immediate steps to rectify the situation and prevent future occurrences.

Case Study 3: Breach of Protection Obligation by Orchard Turn Developments

17. On 6 July 2017, the PDPC imposed a financial penalty of S\$15,000 on Orchard Turn Developments ("**Orchard Turn**"), the property manager of the ION Orchard shopping mall, for failing to make reasonable security arrangements to protect the personal data of its members that were stored on its server.
18. On 26 December 2015, an unknown perpetrator gained access to Orchard Turn's email application using valid account admin credentials, and sent phishing emails to 24,913 of Orchard Turn's subscribers. Upon discovering this data breach, the Information Technology service provider disabled the email server and sent emails shortly thereafter to the subscribers informing them of the phishing emails.

CASE UPDATE



19. The PDPC found a number of problems with Orchard Turn's data protection practices and security arrangements.
20. First, despite Orchard Turn having a separate server (which was not connected to the Internet) designed to retain all personal data (the "LMS Server"), there had been daily automatic transfers from this server to the email server (which was connected to the Internet). Further, Orchard Turn failed to purge the email server of personal data every day, thereby creating a personal store of personal data on it. These practices greatly increased the security risk and were unnecessary, given that email blasts were sent approximately once a month. Instead, Orchard Turn should have transferred personal data from the LMS Server to the email server only when required for sending out emails, and should have promptly deleted the personal data once the emails were sent.
21. Second, there were no policies and practices to safeguard admin account passwords which could be used to access and use personal data. It transpired that four users had been sharing one admin account. This was problematic in making the identification of the source of the leak much more difficult, if not impossible. Further, the password for the admin account had not been changed for more than one year, increasing the risk of the account being compromised.
22. Third, Orchard Turn had failed to regularly patch its email application, creating exposure to known vulnerabilities.
23. Fourth, Orchard Turn had not conducted vulnerability assessments prior to the roll out of its system. This meant that Orchard Turn was not aware of the vulnerabilities of its system, and could not properly determine the technical measures to be taken to ensure that personal data was adequately protected.
24. As a result, the PDPC imposed a financial penalty of S\$15,000 and directed Orchard Turn to to patch all system vulnerabilities already identified, conduct a penetration test and rectify new weaknesses identified, as well as implement a password management policy and conduct training for staff on password management best practices. It also considered the fact that a large number of subscribers were affected, and that the phishing emails had exposed these subscribers to further risks. These facts were balanced against Orchard Turn's cooperation with the PDPC, and its prompt remedial action and corrective measures taken upon discovering the data breach.
25. Organisations that handle large amounts of personal data must ensure that adequate security measures are taken in order to protect the personal data. It would be highly advisable to conduct tests and checks to identify systemic vulnerabilities and weaknesses, and take steps to ensure these vulnerabilities are addressed in ways which would minimize or eliminate risks. In particular, measures should be taken to ensure that potential exposure of personal data is minimized, admin accounts and their passwords are managed securely, and systems which hold personal data are patched regularly. Finally, if a data breach does indeed occur, it is imperative for prompt remedial action to be taken.

Conclusion

26. The PDPC has remained active in its investigations and enforcement. Organisations should ensure that personal data under their control or possession are handled properly and securely. They should also stay abreast of developments in data protection law to understand what to look out for, and what measures to take to ensure compliance with the PDPA.

CASE UPDATE



27. Please do not hesitate to contact us if you have any questions relating to this case update, or require any advice on complying with personal data protection law in Singapore.

About Lee & Lee

Lee & Lee is one of Singapore's leading law firms being continuously rated over the years amongst the top law firms in Singapore. Lee & Lee remains committed to serving its clients' best interests, and continuing its tradition of excellence and integrity. The firm provides a comprehensive range of legal services to serve the differing needs of corporates, financial institutions and individuals. For more information: visit www.leenlee.com.sg.

The following partners lead our departments:

Kwa Kim Li
Managing Partner
kwakimli@leenlee.com.sg

Quek Mong Hua
Litigation & Dispute Resolution
quekmonghua@leenlee.com.sg

Owyong Thian Soo
Real Estate
owyongthiansoo@leenlee.com.sg

Tan Tee Jim, S.C.
Intellectual Property
tanteejim@leenlee.com.sg

Adrian Chan
Corporate
adrianchan@leenlee.com.sg

Louise Tan
Banking
louisetan@leenlee.com.sg