PDPA Compliance by MCSTs

Documents you will need and what can we learn from the non-compliance cases so far

Norainni Rahman
DePO Services LLP

CONTENT

Must MCSTs comply with PDPA?

PDPA non-compliance cases involving MCSTs

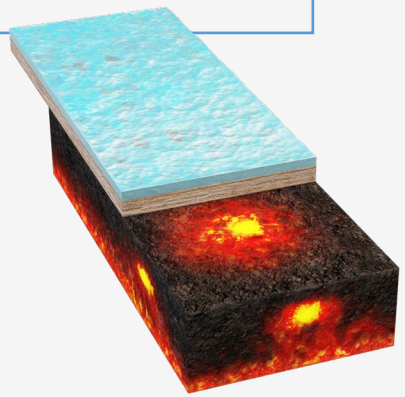
Are Managing Agents liable for MCSTs non-compliance of PDPA?

What is a Data Protection Management Programme (DPMP)?

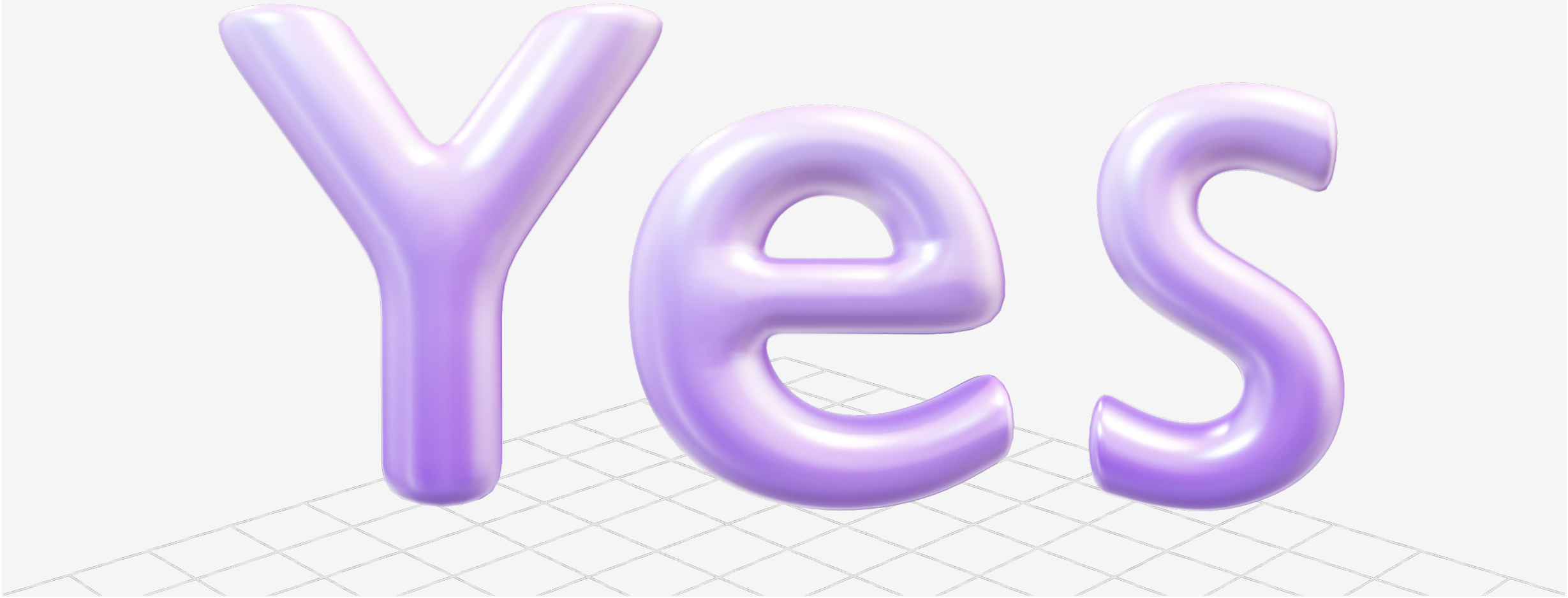
What documents are required under the DPMP?

Should I outsource my DPO functions?

Q&A

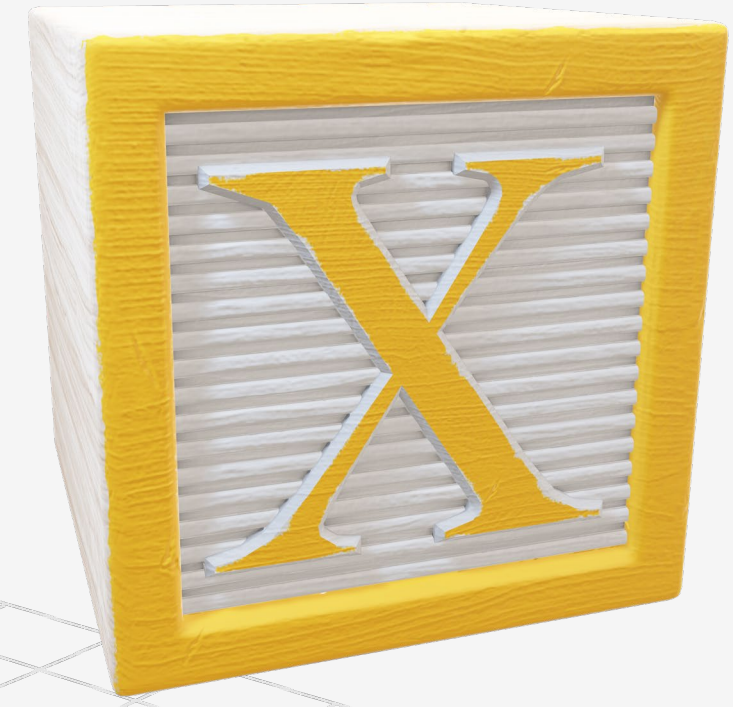


MUST MCSTS COMPLY WITH PDPA?



PDPA NON-COMPLIANCE CASES INVOLVING MCSTS

- Breach of the Protection Obligation by MCST 3400
- Breach of the Protection and Accountability Obligations by MCST 3593 and Breach of the Protection Obligation by New-E Security
- Breach of the Protection and Accountability Obligations by MCST 4375 and Breach of the Protection Obligation by A Best Security Management
- Breach of Protection Obligation by Eagle Eye Security Management Services



BREACH OF THE PROTECTION OBLIGATION BY MCST 3400

- A directory containing personal data belonging to Management Corporation Strata Title Plan No. 3400 (the "Directory") was accessible on the Internet by any member of the public
- Data of 562 individuals collected for the purposes of complying with the Building Maintenance and Strata Management Act, the Building Maintenance (Strata Management) Regulations 2005, as well as to contact subsidiary proprietors.
- MCST failed to put in place reasonable security arrangements to protect the Disclosed Data and was in breach of the Protection Obligation because:
    - It did not conduct code reviews and pre-launch testing6 before new IT features or changes to IT systems are deployed.
    - MCST should have organisations should conduct periodic security reviews of its IT systems.
- It is important for an organisation to be aware of and track its personal data assets. The creation and maintenance of a personal data asset register (i.e. a record identifying all personal data in the organisation's possession or control) is a good practice that would assist organisations to comply with the Protection Obligation.
- Warning issued

BREACH OF THE PROTECTION AND ACCOUNTABILITY OBLIGATIONS BY MCST 3593 AND BREACH OF THE PROTECTION OBLIGATION BY NEW-E SECURITY

- MCST outsource security to New-E. The MA's scope of work as managing agent included supervising New-E to ensure it carried out its duties properly.

- Owner resident requested to New-E CCTV footage. The Requested CCTV Footage had captured images of identifiable individuals who had passed through the common property during that period, and hence contained personal data of those individuals. The Security Supervisor proceeded to review the CCTV recordings and used his mobile phone to record a copy of the Requested CCTV Footage. The Security Supervisor then sent a copy of the Requested CCTV Footage which he had recorded on his mobile phone to the Resident using WhatsApp messenger.

- The footage was posted on the resident's Facebook.

- PDPC found MCST in breach of Sections 11(3), 12 and 24 of the PDPA and New-E in breach of section 24 of the PDPA. I find ETCPM not to be in breach of any of its obligations under the PDPA in relation to the Incident.

BREACH OF THE PROTECTION AND ACCOUNTABILITY OBLIGATIONS BY MCST 4375 AND BREACH OF THE PROTECTION OBLIGATION BY A BEST SECURITY MANAGEMENT

- At the time of the incident, MCST 4375 had appointed Smart Property Management (Singapore) Pte Ltd (“SPMS”) as its managing agent and A Best Security Management Pte Ltd (“ABSM”) to provide security services at the Mall.
- Security CCTV footage of glass door breaking on a person circulated. And finally went up to YouTube.
- MCST replaced Managing Agent.
- PDPC found MCST in breach of PDPA and ABSM in breach of section 24 of the PDPA. It did not find SPMS not to be in breach of any of its obligations under the PDPA in relation to the Incident.
- To the extent that an MCST has appointed a managing agent or vendor to process personal data on its behalf, MCST should have in the agreement with the MA clauses requiring them to comply with the relevant data protection provisions under the PDPA.
- MCST 4375 did not provide any instructions to ABSM or SPMS in relation to requests for access to personal data, as well as the management of CCTV footage in general.

BREACH OF PROTECTION OBLIGATION BY EAGLE EYE SECURITY MANAGEMENT SERVICES

- Leaving the logbook unattended and failing to protect the logbook from prying eyes.
- This was second time there was this breach at the condo.
- 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.
- Eagle Eye was a data intermediary to MCST 3696 (the organisation) in relation to the handling and safekeeping of the logbook.
- Eagle Eye had failed 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.
- 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.

SHOULD I OUTSOURCE MY DPO FUNCTIONS?

Functions of a DPO:

1. Understanding organisation's personal data inventory and reviewing the data management framework and processes to align them with the PDPA.
2. Assessing organisations' policies, procedures and contracts
3. Developing policies for handling personal data in electronic or non-electronic forms, communicating internal personal data policies to customers and handling any queries or complaints about personal data
4. Inform all employees of the organisation's data protection policies and their role in safeguarding personal data
5. Ensure the employees know what the internal processes are with regard to protecting personal data
6. Conduct regular internal audits to ensure that the organisation's processes adhere to the PDPA
7. Assess and alert the organisation of any risk of a data breach or other breaches of the PDPA and to liaise with the PDPC for investigations on breaches, if necessary.

WHAT POLICIES AND PROCEDURES TO DEVELOP?

To ensure compliance with the above requirement, MCSTs need to develop and implement their Data Protection Management Program, which involves the following:

- Data Inventory Map – to track data assets
- Consent Registry
- General Data Protection Policy (Internal) and Personal Data Protection Notices
- Drafting the following Personal Data Protection SOPs for the following:
  - data collection (including withdrawal of consent)
  - data access and correction (including access request and access acknowledgment forms)
  - data protection and data retention (which includes code of conduct in handling and processing personal data of individuals, including third party individuals)
  - data transfer (to outside of organisation); including SOP for Vendors and in Tender exercises

WHAT POLICIES AND PROCEDURES TO DEVELOP?

To ensure compliance with the above requirement, MCSTs need to develop and implement their Data Protection Management Program, which involves the following:

- Data Inventory Map – to track data assets
- Consent Registry
- General Data Protection Policy (Internal) and Personal Data Protection Notices
- Drafting the following Personal Data Protection SOPs for the following:
  - data collection (including withdrawal of consent)
  - data access and correction (including access request and access acknowledgment forms)
  - data protection and data retention (which includes code of conduct in handling and processing personal data of individuals, including third party individuals)
  - data transfer (to outside of organisation); including SOP for Vendors and in Tender exercises

WHAT POLICIES AND PROCEDURES TO DEVELOP? Continued…

- PDPA complaint-handling
- Review of contracts to include DP clauses (Data Protection Agreement)
- Photography, Videography and CCTV Surveillance notices
- Notices where Personal Data is collected
- Data Breach Management Response Plan
- Data Protection Impact Assessment (for new services, new systems or new business activities)

DePO SERVICES LLP RATES

Items	Rate (SGD)	Discounted Rate
Data Inventory Map and setting up of a consent registry	600.00	**1,200.00**
General Data Protection Policy (Internal) and Personal Data Protection Notices	1,000.00	
Drafting the following Personal Data Protection SOPs for each functional unit: - data collection (including withdrawal of consent) - data access and correction (including access request and access acknowledgment forms) - data accuracy - data protection and data retention (which includes code of conduct in handling and processing personal data of individuals, including third party individuals) - data transfer (to outside of organisation); including SOP for Vendors and in Tender exercises - PDPA complaint-handling - Do Not Call Provisions (if required)	3,500.00	
Review of contracts to include DP clauses (Data Protection Agreement)	500.00	
Due diligence checklist in selection of Vendors and Service Providers	400.00	
Photography, Videography and CCTV Surveillance notices	300.00	
Notices where Personal Data is collected	200.00	
Data Breach Management Response Plan	700.00	
Data Protection Impact Assessment (for new services, new systems or new business activities)	500.00	**250.00**
Advisory on Role of a Data Protection Officer	300.00	**150.00**
Annual Review / Internal Audit of PDPA process and practices (for 1st year) (includes report of findings and suggestions for improvements)	1,500.00	**300.00**

Contact Details

DePO Services LLP

Norainni Rahman

LLB (HONS) (NUS)

CIPM | CIPP/A | PCPDPA

norainni@dposervices.net

98362253 (WhatsApp)