ADVISORY GUIDELINES FOR MANAGEMENT CORPORATIONS

ISSUED 11 MARCH 2019

TABLE OF CONTENTS

PART I: INTRODUCTION

1 Introduction

1.1. These Guidelines are developed in consultation with the Building and Construction Authority ("BCA") to provide guidance to management corporations of strata title plans ("MCST") on the Personal Data Protection Act 2012[1] ("PDPA").

1.2. These Guidelines should be read in conjunction with the document titled "Introduction to the Guidelines" and are subject to the disclaimers set out therein. MCSTs are also encouraged to read the other Advisory Guidelines issued by the Personal Data Protection Commission ("Commission") from time to time. These include the Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines"), the Advisory Guidelines on the Do Not Call Provisions, as well as the Advisory Guidelines on the PDPA for Selected Topics.

1.3. These Guidelines clarify how the Data Protection Provisions in the PDPA[2] apply to MCSTs' collection, use and disclosure of personal data, as well as suggest good data protection practices in certain scenarios. They are not meant to exhaustively address every obligation in the PDPA or other laws that would apply in a particular scenario.

1.4. MCSTs are reminded to ensure compliance with other laws, such as the prevailing Building Maintenance and Strata Management Act[3] ("BMSMA"), Building Maintenance (Strata Management) Regulations 2005 ("BMSMR"), and the Land Titles (Strata) Act[4]. The Data Protection Provisions in the PDPA do not affect any obligation or right under other laws (except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA).[5] Further, if there is any inconsistency between another written law and the Data Protection Provisions in the PDPA, the other written law will prevail to the extent of such inconsistency.

---

[1] Act 26 of 2012.
[2] PDPA Parts III to VI.
[3] Cap. 30C
[4] Cap. 158
[5] More specifically, section 4(6)(a) of the PDPA provides that the Data Protection Provisions of the PDPA do not affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law (except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA).

PART II: APPLICATION OF THE DATA PROTECTION PROVISIONS TO SCENARIOS FACED BY MANAGEMENT CORPORATIONS

2 MCSTs and Managing Agents

2.1 A MCST comprises the subsidiary proprietors of all lots within the specific strata title plan (an "estate"), which could be residential buildings such as apartments and condominiums, or commercial buildings such as shopping malls, offices and medical centres. Accordingly, a MCST is considered an organisation[6] under the PDPA.

Collection, use or disclosure of personal data by MCSTs

2.2 MCSTs carry out duties and functions as set out in the BMSMA, for example, to properly maintain the common property. In the course of performing their duties and functions under the BMSMA, MCSTs are required to collect personal data of individuals for a number of specific purposes. For instance, MCSTs are required to collect the name and address of the subsidiary proprietor, the name of any mortgagee of the lot, and the name of the representative of the subsidiary proprietor where such subsidiary proprietor is a company, for the purposes of preparing and maintaining a strata roll.[7] Subsidiary proprietors are also required to give written notice to the MCST of their addresses in Singapore for the service of notices[8], as well as to provide the names and addresses of the proxy giver or proxy holder in the proxy form[9]. Under the BMSMR, MCSTs are required to collect the names, NRIC/FIN numbers and addresses of elected members of the council and executive committee of the MCST.

2.3 If a MCST is required or authorised to collect, use or disclose personal data without consent under the BMSMA, BMSMR or other laws[10], it may do so without obtaining consent from the individual[11]. Otherwise, consent must be obtained in accordance with the PDPA. For example, if the MCST wishes to collect mobile numbers of

---

[6] The PDPA defines an organisation as "any individual, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore".
[7] Please refer to section 46 of the BMSMA.
[8] Please refer to section 65 of the BMSMA.
[9] Please refer to the First Schedule (para 17) to the BMSMA.
[10] As the Singapore Courts have expressed that by-laws passed by the MCST are statutory contracts between the MCST and subsidiary proprietors, i.e. they impose contractual obligations on the respective parties, these by-laws shall not be an excuse for contravening the PDPA as set out under section 4(6)(a) of the PDPA. Further, given that MCST by-laws do not have any legislative effect, they do not constitute "other written law" for the purposes of section 4(6)(b) of the PDPA.
[11] Please refer to section 13(b) of the PDPA. Section 4(6)(b) of the PDPA further provides that the provisions of other written law will prevail to the extent of any inconsistency with the Data Protection Provisions in the PDPA.

subsidiary proprietors for inclusion into the strata roll or other purposes (e.g. issuing car decals), the MCST would have to notify and seek consent from the relevant individuals for the purposes, as the BMSMA[12] does not require such information to be collected in the strata roll. In the case of email addresses, as the BMSMA provides for MCSTs to serve notices to subsidiary proprietors by email (in addition to post)[13], subsidiary proprietors may provide their email address for this purpose, and the email address of subsidiary proprietors may be included as personal data as part of the information in the strata roll for the purpose of serving notices on the relevant subsidiary proprietors. However, if subsidiary proprietors provide their email address to the MCST for purposes such as issuing car decals, consent will need to be sought from the subsidiary proprietor to include the email addresses in the strata roll for other purposes.

2.4	**Example: Disclosure of personal data to subsidiary proprietors** Mary is a resident at estate ABC. Recently, her apartment ceiling started leaking water and she wishes to get in touch with the owner of the unit above hers to resolve the issue. She approaches the MCST to obtain the mobile number of the unit owner. As consent is needed from the unit owner to disclose his mobile number for this purpose, the MCST notifies the unit owner and obtains his consent to disclose his mobile number to Mary for this purpose.

Managing agent as data intermediary

2.5 MCSTs may appoint managing agents to carry out one or more of its duties or functions. Given that managing agents may process personal data on behalf of MCSTs, managing agents may be considered data intermediaries[14] in relation to the personal data that they process on behalf of the MCSTs. A data intermediary that processes personal data pursuant to a written contract[15] will only be subject to the Protection Obligation and Retention Limitation Obligation of the Data Protection Provisions. The organisation for which the personal data is processed (i.e. the MCST) remains responsible for complying with all the Data Protection Provisions. Accordingly, as a

[12] Please refer to section 46 of the BMSMA.
[13] Please refer to sections 46 and 129 of the BMSMA.
[14] The PDPA defines a data intermediary as "an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation".
[15] Please refer to the Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data for more information on sample data protection clauses which may be adopted and included in the agreements between MCSTs and managing agents.

good practice, MCSTs should ensure that it undertakes the necessary due diligence to assure itself that a potential managing agent is capable of complying with the PDPA, and enter into suitable data processing agreements with such managing agent if it contemplates such managing agent to undertake data processing functions on its behalf. Data intermediaries are responsible for complying with all the Data Protection Provisions in respect of other activities which do not constitute the processing of personal data on behalf of and for the purposes of another organisation.

Data Protection Policies and Data Protection Officer

2.6 In complying with the PDPA, a MCST is required to develop and implement policies and practices that are necessary for it to meet its obligations under the PDPA, and to make information about the data protection policies and practices available on request[16]. A MCST is also required to designate at least one individual to be responsible for ensuring its compliance with the PDPA, commonly known as the Data Protection Officer ("DPO")[17].

2.7 Responsibilities of the DPO include:

a. Putting together a personal data protection policy that sets out the purposes for which personal data may be collected, used or disclosed by the MCST as well as other data protection practices of the MCST to ensure compliance with the PDPA[18] and making information about this policy available to all stakeholders[19];

b. Raising awareness and fostering a culture of data protection among staff (e.g. estate security guard), subsidiary proprietors, estate residents and council as well as executive committee members of the MCST;

c. Developing and implementing policies and processes for the proper handling and management of personal data protection related queries and complaints

[16] Section 12(a) of the PDPA.

[17] The MCST should ensure that the individual(s) designated as the DPO is clearly apprised of his or her DPO responsibilities. Please refer to the Commission's website for more information on responsibilities of Data Protection Officers.

[18] For example, to control, administer or manage common property under the BMSMA, MCSTs are reminded to only collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances, and that the individual has been informed of the Purpose Limitation Obligation.

[19] In stating the purposes for which personal data may be collected, used or disclosed in the data protection policy, MCSTs must generally still notify individuals of the purpose and obtain consent at the point of collecting their personal data.

(e.g. access and correction requests) and making information about the complaints process available on request; and

d. Alerting the MCST to any risks that might arise with regard to the collection, use or disclosure of personal data.

2.8 In view that the managing agent of the MCST may be appointed to carry out one or more of the MCST's duties or functions, the MCST may designate an individual within the MCST as its DPO, who may in turn delegate certain data protection duties and functions to the managing agent. The MCST remains fully responsible for complying with the PDPA.

2.9 The following section clarifies how the PDPA applies to common scenarios involving the collection, use or disclosure of personal data by MCSTs, and highlights good data protection practices that could be adopted.

3 Common activities that involve the collection, use or disclosure of personal data

Dissemination of notices containing personal data

Voter List

3.1 Under the BMSMA, MCSTs are required to display a list of the names of the persons who are entitled to vote as well as the addresses of lots owned by these persons on the estate's notice board[20], at least 48 hours before the general meeting. Given that the BMSMA requires the names of persons entitled to vote as well as the lots in respect of which each of these persons is entitled to vote to be displayed on the estate's notice board, consent for the disclosure of such information for such purposes is not required under the PDPA. If MCSTs wish to display additional information other than those specified in the BMSMA, MCSTs are required to obtain consent from the relevant individuals before displaying and disclosing such other personal data, unless an exception applies[21]. MCSTs must also ensure that the disclosure of such other personal data would not be considered excessive or inappropriate. As good practice, MCSTs should take care to display the list of voters for a reasonable duration and not display it for a longer period than necessary (e.g. removing the list of eligible voters soon after the conclusion of the general meeting).

20 Please refer to the First Schedule (para 7) to the BMSMA.
21 Please refer to the Second, Third and Fourth Schedules of the PDPA on the exceptions when organisations may collect, use, or disclose personal data without consent.

3.2	**Example: Voter List** In the lead up to an annual general meeting to vote for the MCST executive committee of estate DEF, the MCST displayed a list of eligible voters on estate DEF's notice board. The list included the names of voters and their email addresses. As the names of voters are required to be displayed on the estate's notice board pursuant to the BMSMA, consent for the disclosure of voters' names is not required. However, consent is needed from residents to disclose their email addresses for this purpose.

Minutes of meeting

3.3 Apart from general meetings of the MCST, MCST councils and executive committees are also required to hold their respective meetings. Under the BMSMA, the council or executive committee of the MCST is required to "cause minutes of general meetings to be kept" [22], as well as keep "full and accurate minutes" of its proceedings[23]. Since the function and purpose of the minutes of meetings are to accurately record what happened at the meeting, the minutes could include the personal data of estate residents or invitees to identify and record the persons in attendance[24] or arising from discussions on matters relating to these individuals during the meetings. Further, the council or executive committee must display a copy of the minutes of its meeting as well as the minutes from the MCST's general meeting on the estate's notice board for a period of not less than 14 days.[25] The council may also give each subsidiary proprietor a copy of the minutes after the meeting.[26] Personal data captured in the minutes may therefore be disclosed as a consequence. As a good practice, MCSTs should take care to display the minutes of meeting for a reasonable duration and not display it for a longer period than necessary.

3.4 As good practice, MCSTs should notify all subsidiary proprietors and estate residents (particularly new residents) that their personal data will be collected for the dissemination of the minutes of meetings and the voter list in accordance with the BMSMA. This could be done through the MCST's personal data protection policy, or notice of general meeting.

---

[22] Please refer to Second Schedule (para 3) to the BMSMA.
[23] Please refer to the First Schedule (para 10A) to the BMSMA for minimum mandatory information required to be recorded in the minutes of general meetings.
[24] *Re Exceltec Property Management Pte Ltd and others* [2017] SGPDPC 8.
[25] Please refer to Second Schedule (para 3(2)) of the BMSMA.
[26] Please refer to Second Schedule (para 3(4)) to the BMSMA.

3.5	**Example: Minutes of Meeting** Following estate GHI's MCST general meeting, the council posted the minutes of meeting on the notice board in the estate as required under the BMSMA. The minutes recorded the discussion surrounding a complaint made by one of the residents in the estate, against another resident. The resident noticed that her name and unit number was disclosed in the minutes, and asked the MCST council about this. The MCST explained to the resident that the BMSMA requires full and accurate minutes of the meeting to be captured and posted. All subsidiary proprietors and residents of estate GHI had also been informed of this requirement through the MCST's personal data protection policy that is available on its website.
3.6	**Example: Recording of proceedings to ensure full and accurate minutes of meeting** For estate GHI's MCST general meeting, MCST council members wish to take audio recordings of the proceedings of general meeting for the purpose of ensuring that full and accurate minutes of the meeting are captured. As audio recordings may capture more personal data than is necessary for the recording of full and accurate minutes of meeting, the MCST must notify subsidiary proprietors and residents, such as through the MCST's personal data protection policy or notice of general meeting, that audio recordings of the proceedings will be taken during the meeting. Deemed consent for such audio recordings to be taken would be considered to have been given by the attendees of the meeting. The MCST should only use the audio recordings for the purpose of ensuring that full and accurate minutes of meeting are captured. While there are no provisions in the BMSMA that address this issue, the MCST must comply with other Data Protection Provisions of the PDPA.

Handling access and correction requests

3.7 Under the PDPA, MCSTs are required to provide access to or make a correction to the individual's personal data in the MCSTs' possession or under their control upon the individual's request, unless a relevant exception under sections 21 or 22 of the PDPA

applies[27]. For example, MCSTs must provide access to an individual's personal data captured in close-circuit television camera ("CCTV") footage requested by the individual, unless an exception applies. To be clear, MCSTs may not limit the provision of access to personal data only to law enforcement or other relevant authorities, or for the purposes of investigations by such authorities. To this end, MCSTs must develop and implement policies and processes for handling access and correction requests to ensure compliance with the PDPA.

3.8 MCSTs must also respond to an access request (i.e. provide access to the personal data) as soon as reasonably possible from the time the access request is received. If a MCST is unable to respond to an access request within 30 days after receiving the request, the MCST must inform the individual in writing within 30 days of the time by which it will be able to respond to the request. MCSTs may charge a reasonable fee for providing the requested access that reflects the time and effort required to respond to the access request.

3.9 While the PDPA does not require that an access request be accompanied by a reason for making the request, as good practice, MCSTs could ask the applicant to be more specific as to what type of personal data is required, as well as the time and date the personal data was collected, to facilitate processing of the access request, or to determine whether the request falls within one of the prohibitions under section 21(3) of the PDPA or any exception in the Fifth or Sixth Schedule. MCSTs could also ask the applicant as to what form a CCTV footage extract could be provided in (e.g. screenshot or video footage), in order to fulfil the access request in the most cost efficient manner.

3.10 In situations where access and correction requests are handled by managing agents, MCSTs should establish clear policies and processes for the handling of access and correction requests by these managing agents to ensure compliance with the PDPA.

3.11 Please refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA for further information relating to the Access and Correction Obligations, and the Guide to Handling Access Requests for more information on how organisations should respond to access requests.

[27] If the organisation determines that it is appropriate under section 21 of the PDPA and Part II of the Personal Data Protection Regulations 2014 to not provide some or all of the personal data requested, the organisation should keep the withheld personal data for a reasonable period – minimally 30 calendar days or longer after rejecting the access request – as the individual may seek a review of the organisation's decision.

3.12	**Example: Access request for personal data in CCTV footage that no longer exists** John is a resident at estate JKL. He wrote to the estate's MCST to request for access to the CCTV footage of himself on the estate's premises on a certain date and time. However, as the CCTV system only retained recorded CCTV footage for a period of 14 days, John's requested footage was no longer available at the time of the access request. Nonetheless, the MCST did not respond to John's request to inform him that the requested footage of the incident was no longer available. Section 21(1) of the PDPA requires the MCST to provide John with his requested personal data unless an exception applies. In this case, a possible exception applies[28] as the requested footage has been deleted prior to the request. The MCST must provide a reply to John even if it is not providing access to the requested personal data, and as good practice, inform John of the relevant reasons for rejecting his access request. The MCST should also have in place a retention policy that sets out when the MCST ceases to retain personal data contained in the CCTV footage.
3.13	**Example: Access request for CCTV footage capturing personal data of other individuals** Sarah is a resident at estate MNO. She wrote in to the estate's MCST to request for access to the CCTV footage that captures her, as well as other individuals, in the residents' private gym on a certain date and time. In providing Sarah with access to the requested personal data, the MCST should generally ensure that Sarah only has access to her own personal data captured in the CCTV footage, for example, by applying appropriate masking of the personal data of other individuals in the footage. The MCST may provide Sarah access to the requested CCTV footage without masking the other individuals' personal data, only if the other individuals have provided consent for the disclosure of their personal data for this purpose or if the disclosure is pursuant to an exception under the Fourth Schedule to the PDPA[29].

[28] Paragraph 1(j)(iii) of the Fifth Schedule to the PDPA.

[29] This includes, amongst others, situations where the disclosure is necessary:

(a) for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way; or

(b) to respond to an emergency that threatens the life, health or safety of the individual or another individual.

	The MCST could also consider if providing photo stills of the CCTV footage would meet Sarah's request.

Estate security

Visitors and invitees

3.14 The personal data of visitors and invitees (such as subcontractors) may be routinely collected for security purposes. This may be done in various ways. For instance, visitors may be required to provide certain personal data to estate security, such as his or her name, vehicle number (where relevant), contact details and the unit number which he or she is visiting, by filling in a visitor log book at the guard house of a condominium or the reception desk of a commercial building, before being allowed to enter. There may also be CCTV images captured[30] of the visitors and invitees.

3.15 MCSTs should only collect personal data that is necessary for the purpose and avoid collecting excessive personal data, taking into consideration what a reasonable person would consider appropriate in the circumstances. Ordinarily, having sight of a visitor's photo identification and recording the visitor's name and contact details (e.g. mobile number) would be considered reasonable for a condominium's security purposes. In exceptional circumstances, where a MCST assesses that the failure to accurately identify the visitor or invitee to a high degree of fidelity will pose significant security risks, it may be reasonable for the MCST to record the NRIC numbers of visitors to accurately establish and verify the identity of the individual. The MCST must be able to justify the recording of the NRIC numbers of visitors or invitees. Please refer to the Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers for more information.

3.16 The MCST must also comply with the obligation in the PDPA to make reasonable security arrangements to protect the personal data of visitors or invitees from unauthorised use or disclosure. In doing so, MCSTs should take into consideration the nature of personal data, the form in which the personal data has been collected (i.e. physical or electronic), and the possible impact to the individual concerned if an

[30] MCSTs may also install CCTVs at common areas around the estate to ensure the security of the estate. Given that CCTVs collect personal data of individuals in the estate, MCSTs must ensure compliance with the PDPA obligations. To fulfil their obligation to obtain consent to collect, use or disclose personal data captured by CCTVs, notices may be placed within the estate premises (e.g. entrance or prominent locations in the estate) to indicate the operation of CCTVs for security purposes. Please refer to Chapter 4 of the Advisory Guidelines on the PDPA for Selected Topics for an elaboration on how the PDPA applies in general to activities relating to CCTVs.

unauthorised person obtained, modified or disposed of the personal data. For example, a MCST that collects the name and NRIC numbers of invitees must have in place a greater level of security to protect such personal data (e.g. employing a visitor management system with appropriate technical measures to control access). This is in view of the risk to individuals if NRIC numbers, which could be used to unlock large amounts of information relating to the individual, were obtained and used for illegal activities such as identity theft and fraud.

3.17	**Example: Collection of visitor's personal data** Amber is visiting a friend at estate PQR. The security guard at the entrance notifies her of the need to record her vehicle number and contact details, for security purposes. She fills in the visitor log book accordingly. Amber is deemed to have consented to the collection, use or disclosure of her personal data under the PDPA.
3.18	**Example: Collection and care of visitor's NRIC numbers** Brandon is visiting a data centre at STU building. At the reception counter of building, he is asked to fill in his NRIC number, name and contact details in a visitor log book. While doing so, he is able to see the NRIC numbers, names and contact details of all the other visitors. The visitor log book is placed on the counter, open and facing all visitors at the counter. The MCST of STU building has assessed and is able to justify that the collection of NRIC numbers is necessary to accurately establish and identify the identity of every visitor or invitee entering STU building to a high degree of fidelity as the failure to do so will pose significant security risks. The MCST should adopt appropriate security arrangements that would meet the higher level of protection that is required, such as implementing an electronic visitor management system and/or activating auto screen lock mechanisms for the computer screen if left unattended.
3.19	**Example: Collection of visitors' partial NRIC numbers** Jasmine is visiting a friend at estate VWX. The security guard at the entrance notifies her of the need to fill in the visitor chit with her name, contact number and partial NRIC number (i.e. last three digits and checksum of her NRIC number), for security purposes. After Jasmine fills in the visitor chit, the security guard checks her physical NRIC to verify the name and partial NRIC number provided. In this case, the MCST of VWX is not considered to have collected Jasmine's NRIC number. Nonetheless, the MCST must still comply with the Data Protection Provisions

	of the PDPA, including making reasonable security arrangements to protect the personal data of visitors or invitees from unauthorised use or disclosure.

Subsidiary proprietors

3.20 Typically, estate residents in a residential building, and/or certain invitees of a commercial building (such as employees of an occupier), may enter and leave the estate premises using access cards. In the application for access cards and/or the maintenance of the access cards system, MCSTs may require the contact details (i.e. names, telephone numbers and email addresses) of the individuals who hold access cards.

3.21 MCSTs must ensure that the individuals provide their consent (or deemed consent) for the collection, use or disclosure of their personal data for the purpose of providing them access through the use of access cards, in compliance with the PDPA.

Photographs or video recordings of social activities

3.22 From time to time, MCSTs may organise social functions or activities for estate residents. Where MCSTs intend to take and use photographs or video recordings of estate residents, visitors or invitees attending these events for a purpose, MCSTs must notify and obtain consent from these individuals to collect, use or disclose their personal data for the purpose. For example, organisers of social activities should notify participants that photographs of them may be taken at the event for the purpose of publishing them in an estate newsletter or annual general meeting presentation, and provide information about how they may withdraw consent.

3.23 The Data Protection Provisions do not prescribe the ways in which consent may be obtained. MCSTs may do so in the most effective way depending on the circumstances. In some instances, consent may be deemed to have been given when the individual has been notified that a video recording will be made at an event and the individual voluntarily participates in the event, or the individual voluntarily permits a photograph or video recording to be taken of him or her.

3.24 More information on how individuals may be notified of the purposes for the collection, use or disclosure of their personal data can be found in the Guide to Notification.

3.25	**Example: Posting photographs of estate residents for events** The MCST of estate XYZ organised an annual private poolside party for estate residents. The MCST intends to post photographs of the residents who were at the party on the estate's website and notice board after the party. In this case, the MCST could clearly state in its invitation to residents that photographs of residents will be taken at the party for the purpose of publication on the estate's website and notice board, and provide a way for residents to withdraw consent if they wish to. Alternatively, the MCST could put up an obvious notice at the entrance of the event venue to notify residents that photographs will be taken at the event for such purposes. Please refer to Chapter 4 (Photography, Video and Audio Recordings) of the Advisory Guidelines on the PDPA for Selected Topics for an elaboration on how the PDPA applies to activities relating to photography.

4 Protection and retention of personal data

4.1 The BMSMA does not prescribe the measures that MCSTs and managing agents[31] should adopt to secure personal data in their possession or under their control. For example, the visitor log book, access card system, facilities log book, documents containing residents' feedback or complaints, and resident's portal are likely to contain personal data. Therefore, MCSTs and managing agents must comply with the Data Protection Provisions in the PDPA, and make reasonable security arrangements[32] to protect such personal data in their possession or under their control to prevent accidental or unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Security arrangements may take various forms such as administrative measures, physical measures, technical measures or a combination of these. Please refer to Chapter 17 of the Advisory Guidelines on Key Concepts in the PDPA for more details on the considerations that apply in relation to the Protection Obligation, as well as examples of administrative, physical and technical measures.

4.2 MCSTs and managing agents must also have in place a retention policy that sets out when they cease to retain documents containing personal data (e.g. visitor entries in the log book)[33]. Under the Retention Limitation Obligation, the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals (i.e. anonymise the data) as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and the retention of personal data is no longer necessary for legal or business purposes. In doing so, MCSTs and managing agents must ensure that there is proper and secure disposal of personal data.

4.3 In this regard, as part of their retention policies, MCSTs and managing agents may retain all records, books of account and such other documents relating to any transactions or operations for a period of not less than 5 years from the end of the financial year in which the transactions or operations to which those documents relate are completed, as required by the BMSMA.[34] Beyond this period of retention, MCSTs

[31] A managing agent, being a data intermediary that processes personal data on behalf of a MCST, will be subject to the Protection Obligation and Retention Limitation Obligation of the Data Protection Provisions.
[32] Please refer to section 24 of the PDPA.
[33] This could be when the purpose for which that personal data was collected is no longer being served by retention of personal data, or when retention is no longer necessary for legal or business purposes (section 25 of the PDPA).
[34] Please refer to section 48(2) of the BMSMA.

and managing agents should assess on a standard of reasonableness, whether the purposes for which the personal data was collected is served, or if there are other legal or business purposes for which retention of the personal data may be necessary.[35]

4.4 Please refer to the Guide to Disposal of Personal Data on Physical Medium and the Guide to Securing Personal Data in Electronic Medium for more information on good practices for disposing personal data in physical forms and protecting electronic personal data.

4.5	**Example: Documents containing personal data** The MCST of estate ABC requires all visitors to record their name, contact details and vehicle licence plate number (where relevant) in the visitor log book located at the security guardhouse situated at the entrance of the estate. The MCST has engaged security staff to be present at the guardhouse around the clock. However, a regular visitor to the estate observed that there were several instances where the guardhouse was left unattended by the security staff, and the visitor log book, which contains personal data of visitors, was left unattended for anyone to access during these periods. The MCST is required to comply with the obligations in the PDPA, including making reasonable security arrangements to protect the personal data in its possession or under its control from loss, misuse or unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Residents or visitors to the estate should not be able to access the personal data of other visitors in the visitor log book, and the MCST should ensure that the visitor log book is kept in a secure place that is only accessible to authorised personnel. In addition, the MCST should have in place a personal data retention policy that governs when it should cease to retain documents such as entries in the visitor log book, which are likely to contain personal data. When ceasing to retain these documents, the MCST would also need to establish processes to ensure the proper and secure disposal of these documents.

[35] Please refer to Chapter 18 of the Advisory Guidelines on Key Concepts in the PDPA for more details on the considerations that apply in relation to the Retention Limitation Obligation.

	For the avoidance of doubt, if the security staff are appointed or engaged as data intermediaries to process[36] personal data on behalf of and for the purposes of the MCST, the security staff processing personal data on behalf of and for the purposes of the MCST pursuant to a contract which is evidenced or made in writing will only be subject to the Protection Obligation and Retention Limitation Obligation while the MCST remains fully responsible for complying with all the Data Protection Provisions.

END OF DOCUMENT

[36] Section 2 of the PDPA provides that "processing" of personal data means the carrying out of an operation or set of operations in relation to the personal data, and includes any of the following: recording, holding, organisation, adaptation, alteration, retrieval, combination, transmission, erasure, or destruction.