[2017] PDP Digest

PERSONAL DATA PROTECTION DIGEST

pdpc

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

PERSONAL DATA PROTECTION DIGEST

Editor

Yeong Zee Kin

Deputy Editors

David N Alfred

Chen Su-Anne

Jansen Aw

Editorial Assistants

Deborah Lee

Charis Seow

Janice Lee

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

2017

CITATION
This volume may be cited as:
[2017] PDP Digest

Published by Academy Publishing

Academy Publishing is a division of the Singapore Academy of Law.

The Singapore Academy of Law is the promotion and development agency for Singapore's legal industry. Its vision is to make Singapore the legal hub of Asia. It aims to drive legal excellence through developing thought leadership, world-class infrastructure and legal solutions. It does this by building up the intellectual capital of the legal profession by enhancing legal knowledge, raising the international profile of Singapore law, promoting Singapore as a centre for dispute resolution and improving the efficiency of legal practice through the use of technology. More information can be found at www.sal.org.sg.

Communications and Outreach
Personal Data Protection Commission
460 Alexandra Road
#10-02 PSA Building
Singapore 119963
E-mail: info@pdpc.gov.sg
www.pdpc.gov.sg

MCI(P) 092/07/2017

FOREWORD

BY THE CHIEF JUSTICE

In some jurisdictions, data protection is an established area of law and legal practice. In Singapore, however, our Personal Data Protection Act ("PDPA") was enacted only recently in 2012. Data protection law is therefore still in its infancy here. Yet, it is a critically important area of law and we can expect that it will take centre stage in the new digital economy with the increasing adoption of intelligent systems. Artificial Intelligence ("AI") will become more pervasive, even as it becomes less evident to users. Underpinning the effective deployment of AI technology are models that are built with the use of large datasets, including much personal data.

It is unsurprising then that jurisdictions around the world are gearing up for this next industrial revolution by either updating existing or introducing new data protection laws. Recent legislative activities in the region include the enactment of rules and regulations in September 2016 to implement the Philippines' Data Privacy Act; while in Japan, the amended Protection of Personal Information Act took effect in May 2017. Companies around the globe are getting ready for the EU General Data Protection Regulation which takes effect in May 2018. Additionally, Australia has introduced an amendment to its Privacy Act in the Privacy Amendment (Notifiable Data Breaches) Act 2017; and Canada is soliciting feedback on a discussion paper on potential enhancements to consent under the Personal Information Protection and Electronic Documents Act. With the proliferation of domestic data protection laws in many jurisdictions, there will be greater need for the harmonisation of data protection laws to ensure that businesses that operate with a footprint across multiple jurisdictions are able to manage their legal and regulatory compliance without incurring disproportionate operating costs. I expect that cross-border data protection principles like the APEC Cross-Border Privacy Rules will play an increasing role in bridging different domestic data protection systems.

This therefore is an exciting area of law. What makes data protection law especially significant for Singapore and for our legal sector in particular is the opportunity it presents to forge a regime that is suited to our local context thus helping to ensure the competitiveness of our economy. Further, with the growing recognition of the need to govern the processing of data across borders and to ensure interoperability of data protection laws,

Singapore has the chance to contribute to these international developments and influence their trajectory.

It therefore gives me great pleasure to pen this foreword for the Personal Data Protection Commission's inaugural Digest, which I believe will make a valuable contribution to our jurisprudence on data protection. The Digest provides a comprehensive collection of Singapore's data protection enforcement decisions since the PDPA came into effect. Further, the Digest includes a number of articles that discuss specific areas relating to data protection practice, which I expect will be of particular interest to the legal community. The Digest therefore makes a timely and important contribution in this developing area.

I would also like to commend the collaborative efforts of the private sector, academia and Academy Publishing in coming together to contribute to this discourse on data protection law. In particular, I am delighted by the contributions featured in this volume, all of which unquestionably required significant time and effort. This generous sharing of experiences, analyses and suggestions for practical compliance is important for the development of data protection law in Singapore.

Sundaresh Menon

Chief Justice

Singapore

FOREWORD

BY MINISTER FOR COMMUNICATIONS AND INFORMATION

In this next phase of our economy, data plays centre stage. The ubiquity of wearables, sensors and the Internet of Things will make the collection of data ever easier and ever more prevalent. Businesses in Singapore that seek to be part of this new economy have to ensure that good data protection practices are adopted so as to develop and maintain a high level of consumer trust. Forward-looking companies can capitalise on their adoption of good data protection practices as another way to differentiate themselves and to stand out from their competitors. All companies have to work hard to establish Singapore as a trusted hub where companies practise high levels of data protection compliance in order to secure Singapore as a reputable place to anchor businesses.

Indeed, the need to establish a baseline of data protection benchmarked against global leading jurisdictions was one of the key concerns that eventually led to the development of Singapore's Personal Data Protection Act ("PDPA") in 2012.

It will soon be three years since the PDPA came fully into effect. The Personal Data Protection Commission has continued in its active educational efforts and has also been progressively increasing its investigations and enforcement of the legislation. The grounds for finding an organisation in contravention of its data protection obligations are published on the Commission's website as well as other platforms to increase awareness of the common breaches and the reasons leading to such breaches.

But this only tells part of the story.

For every case where a breach is established after investigations, there are others where the organisation is exonerated because they had adopted acceptable standards. These decisions should also be made available because they provide good learning points.

Therefore, it is timely that, in addition to the case decisions where organisations have been found in breach of the PDPA, this Digest makes available the summaries of several cases where organisations have been found to be not in breach of the PDPA pursuant to the Commission's

investigations. These summaries contain useful pointers and highlight the nuances in the interpretation and application of the PDPA. These will aid in the understanding of our data protection legislation, particularly the balance that the legislation seeks to strike between the rights of individuals and the needs of businesses.

The Digest also contains articles that are contributed by data protection practitioners, and their insights on tackling real world data protection issues. Readers can look forward to a collection of articles and viewpoints of these practitioners covering a spectrum of topics from tracing the genesis of Singapore's PDPA to surveying international laws and recent significant international developments especially given growing cross-border data flows. Several articles also explore in greater detail specific aspects of the PDPA, as well as suggest practical approaches to compliance, that may be particularly helpful for organisations to consider when they wish to engage in multifarious personal data activities.

I believe this Digest ultimately aids in facilitating the practical understanding of the PDPA and will contribute to an even more robust data protection ecosystem in Singapore.

Dr Yaacob Ibrahim

Minister for Communications and Information

CONTENTS

Grounds of Decision

Re K Box Entertainment Group Pte Ltd and another

Case Number: DP-1409-A100
Decision Citation: [2016] SGPDPC 1

Data intermediary *– "Processing" of personal data*
Openness Obligation *– Lack of data protection policies and practices – Failure to appoint data protection officer*
Protection Obligation *– Access to personal data – Insufficient technical security arrangements*

20 April 2016

BACKGROUND

1 K Box Entertainment Group Pte Ltd ("K Box") operates a chain of karaoke outlets in Singapore. Finantech Holdings Pte Ltd ("Finantech") is a third-party information technology ("IT") vendor, which is owned and managed by its sole director, [redacted] ("Mr G").

2 On 16 September 2014, the website "The Real Singapore" ("TRS") published a post which indicated that a list containing personal data of about "317,000" K Box members ("List") had been disclosed online at <http://pastebin.com/bnVhn3mp> ("pastebin.com").

3 The List contained personal data which all customers who sign up for a K Box membership, both before and after 2 July 2014, are required to provide, namely:

(a) name (as *per* NRIC);
(b) NRIC / Passport / FIN number;
(c) mailing address (Singapore only);
(d) contact number;
(e) e-mail address;
(f) gender;
(g) nationality;
(h) profession; and
(i) date of birth.

4 After receiving complaints from members of the public regarding the data breach, the Personal Data Protection Commission ("Commission") commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether there had been a breach by K Box and/or Finantech of their respective obligations under the PDPA.

MATERIAL FACTS AND DOCUMENTS

K Box's relationship with Finantech

5 As at 16 September 2014, K Box had engaged Finantech through the "website revamp contract dated 2012" and the "webhosting and server management contract dated 2009" to develop K Box's Content Management System ("CMS") from the ground up and to revamp, manage and host its website. What the parties referred to as "contracts" were actually quotations sent by Finantech to K Box for their confirmation and acceptance. K Box's CMS stored and processed the personal data of its members. The CMS also utilised FCKEditor – a software library component which allowed the user to input formatted text.

6 Mr G of Finantech was the only one who had direct and full access to all the K Box members' personal data as the sole administrator of K Box's CMS. In the past, a former project manager of Finantech, [redacted] ("Mrs G"), whose role was to help Mr G in managing K Box's customer data, also had access through the administrative account in the CMS, *ie* the "admin" account with the password "admin".[2] Mrs G left Finantech in or around 2013. Apart from that, no one else, not even K Box's IT manager [redacted] ("Mr C") or K Box's Chief Operation Officer, [redacted] ("Ms N"), had direct access to the database.

7 K Box employees with the title "Captain" and above[3] (of which there were about 75 people with such a title) had restricted access to a function that allowed viewing of members' personal data such as name, package,

1 Act 26 of 2012.

2 Mr G was the only employee at the material time of Finantech. Mrs G was the only person assisting Mr G in the past.

3 The Captain is the supervisor of the service crews and his role is to access the customers' information to check their booking.

booking date and time, contact number, members' number and visit date and time to check and confirm members' bookings. However, they could only view the details of each member one at a time, and not extract the entire members' list. As such, whenever K Box required members' personal data with selected criteria for marketing and promotional purposes, they would have to inform Mr G of the data required and he would perform the relevant queries on the database, export the information to an MS Excel document and e-mail the document (unencrypted) via Gmail to K Box's IT manager, Mr C, who would in turn e-mail the document to K Box's marketing department via Gmail. During investigations, it was discovered that Finantech had once sent K Box over 90,000 members' personal data via unencrypted e-mail via Gmail. By its own admission, K Box had never instructed Finantech to password-protect or encrypt e-mails containing a large volume of personal data prior to 16 September 2014.

K Box's protection measures

8 According to K Box, measures that were reasonable and appropriate taking into account "the nature of the K Box's business (*ie* value for money, family-orientated, karaoke entertainment for everyone) and the fact that the data are non-financial in nature" were adopted with regard to the security of its members' data.

9 K Box represented that secure server practices such as access controls and data protection policies that were established and observed in the organisation whether before 2 July 2014 or between 2 July 2014 and 16 September 2014 had been put in place since the implementation of its current website to protect individuals' personal data. In addition, K Box represented that before 16 September 2014, employees were required to set alphanumeric passwords consisting of eight alphabets/numbers, one capital and one special case in accordance with K Box's password policy. However, Mr C admitted that K Box did not "conduct audit on whether the staff really use eight numbers/letters alphanumeric, one capital and one special case password [*sic*]" and Mr G had noted a receptionist using a one-letter password in the past. A software system "to force employees to adopt passwords that adhered to the KBox's password policy [*sic*]" was only implemented in November 2014.

10 Although K Box had outsourced its website maintenance, which includes maintenance of its backend CMS, and web hosting of its website

to Finantech ("Services"), K Box represented that Finantech agreed and undertook that it would keep K Box's data confidential as it was a term in their agreements. K Box had also held regular meetings with Mr G/Finantech on all aspects of the Services including any IT security concerns and Finantech would not conduct any major works or modification to the Services without first consulting K Box. K Box had "no reason to doubt" the competence or integrity of Finantech or that Finantech would not comply with the security measures and undertaking. However, by Finantech's own admission, Finantech did not do any system monitoring in terms of IT security, security testing or regular IT security audits at the time of the breach and prior to 17 September 2014.

11 K Box had also represented that it did not have a data protection officer ("DPO") since 2 July 2014 to 20 April 2015 and conceded that its privacy policy prior to 16 September 2014 was not comprehensive. While each employee's employment contract contains a term to keep all information relating to the operations of K Box confidential, there was no policy and physical or online security system in place to monitor whether a staff removed personal data from its premises.

12 In this connection, the "contracts" between K Box and Finantech did not include any contractual clauses that required Finantech to comply with a standard of protection in relation to the personal data transferred to it that is at least comparable to industry standards. According to Finantech's representations, K Box had also never emphasised the need for data protection and their obligation towards K Box under the PDPA or informed Finantech of its data protection obligation after September 2014. Mr G had also represented that while he was aware of the existence of the PDPA, he was not aware of the specifics of it.

The List

13 On 16 September 2014, the same day that TRS published the post mentioned at [2] above, K Box's management realised, via the "Social Media, employees and The Real Singapore website", that K Box members' personal data had been uploaded on pastebin.com. Mr C had also received a call on his mobile phone from an unknown person to inform him that TRS had "posted information of K Box members" and to ask him to verify whether the information belonged to its members. Mr G investigated the breach by matching the disclosed personal data in the List with the

information of K Box's members from its database and confirmed that the List matched the one in K Box's database. Thereafter, K Box notified its members of the data breach by way of a letter dated 16 September 2014 that was published online on the K Box homepage.

14 The next day, 17 September 2014, Mr C "deleted all the accounts of the staff who left [*sic*]" and the unauthorised "admin" account with the weak password "admin" was "deactivated", "disabled" and the "password to the account was changed". The CMS user activity log showed that Mr C had removed 36 accounts on 17 September 2014.

No conclusive evidence that data breach occurred before 2 July 2014

15 Although the List was uploaded on pastebin.com on 16 September 2014, the List only contained members' data up to 23 April 2014. There is no evidence available to conclusively ascertain when the List was obtained.

16 Based on Finantech's initial investigation on the day the List was published, Finantech deduced that the List containing the personal data of K Box members could have been obtained by the cyber-attacker on or around 23 April 2014 for the following reasons:

(a) the List stopped at the member record that was created on 23 April 2014 at 5.43am;

(b) the CMS's "user activity 2014.csv" ("User Activity Log File") recorded that someone had logged in using the "admin" account on 23 April 2014 at 9.59am;

(c) a new member record was created on 23 April 2014 at 12.17pm but this was not included in the List; and

(d) subsequent member records created after 23 April 2014 were also not included in the List.

17 The User Activity Log File recorded that the user of the "admin" account had logged in on 23 April 2014. The "admin" user account was the account used by Finantech's former employee, Mrs G. However, given that Mrs G had already left Finantech in or around 2013 and there was no evidence to suggest that she had been remotely accessing the "admin" account, any use of this account after Mrs G had left Finantech would likely have been unauthorised and could be taken to be done by the cyber-attacker.

18 While it is possible that the data breach occurred on or around 23 April 2014, as there was evidence of unauthorised access to K Box's CMS in April 2014 or even earlier in 2013, the Commission is of the view that further data breaches could also have occurred in the following months until the new CMS was put in place in November 2014 for the following reasons:

(a) the message "Remote session from client name a exceeded the maximum allowed failed logon attempts [*sic*]. The session was forcibly terminated", indicating that more than 240 attempts were made *in a single day*, appeared frequently in the operating system log ("System Log"). The frequency of these messages may indicate unsuccessful attempts to hack into the operating system. The messages started appearing as early as October 2012 and *continued until the latest parts of the log file in September 2014*; and

(b) Finantech itself noted that the System Log showed that the "[unauthorised user of the 'admin' account] *was used to login a number of times after the breach.* However, there was no indication that he had modified any user data". The Commission has reviewed the System Log and the unauthorised user of the "admin" account had performed about 83 logins in the period from 25 February 2014 to 16 September 2014, and about 15 logins in the entire calendar year 2013.

Probable cause of breach

19 While the List only contains members' data up to 23 April 2014, given the number of times the unauthorised user of the "admin" account had logged in to K Box's CMS, it is possible that the cyber-attacker had accessed K Box's CMS after 2 July 2014 when the data protection provisions in the PDPA came into effect, but chose to publish the List reflecting the members' list as at 23 April 2014.

20 Finantech had hypothesised that someone hacked into K Box's CMS using the "admin" user account with the "admin" password and planted a malware control and command centre to retrieve and export the members' data. K Box similarly represented that Mr G had informed Mr C that the breach occurred because "he suspected someone used admin user account with the password also admin to login [*sic*]" and "[Mr G] told me there was

a Trojan in the hosting server and he suspected that was how the leak occurred [*sic*]".

21 While the System Log showed unauthorised usage of the "admin" user account in 2014 and files detected as malware were found in the CMS folder, the Commission has not been able to conclusively verify Finantech's hypothesis even after analysing the User Activity Log File and System Log. Nonetheless, the Commission considers that the "admin" user account, which had a weak password "admin" was one of the possible ways that the data breach could have occurred.

22 Having reviewed the relevant facts and circumstances, including the statements and representations made by K Box and Finantech, the Commission has completed its investigation into the matter, and sets out its findings and assessment herein.

COMMISSION'S FINDINGS AND ASSESSMENT

Issues for determination

23 The issues to be determined in the present case are as follows:

(a) whether K Box had breached its obligation under s 24 of the PDPA ("Protection Obligation");

(b) whether K Box had breached its obligation under ss 11 and 12 of the PDPA ("Openness Obligation"), specifically, ss 11(3) and 12(*a*), for failure to appoint a DPO and put in place privacy policies and practices in contravention of those sections of the PDPA;

(c) whether Finantech is a data intermediary of K Box; and

(d) whether Finantech had breached the Protection Obligation.

Issue A: Whether K Box had breached the Protection Obligation

24 Section 24 of the PDPA states:

> **Protection of personal data**
>
> **24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

25 Pursuant to s 24 of the PDPA, K Box, being an organisation which had its members' personal data under its possession and/or control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risk. The Protection Obligation applies equally to all personal data in the possession or under the control of the organisation, including personal data that the organisation may have collected before 2 July 2014, when the data protection provisions under Pts III to VI of the PDPA came into effect.

26 Following a careful assessment of the relevant facts and circumstances, the Commission is of the view that K Box had not discharged the Protection Obligation under s 24 of the PDPA. There are sufficient grounds (whether each on its own or altogether) to show that K Box failed to make reasonable security arrangements to protect the personal data in its possession or under its control from 2 July 2014 to November 2014. In particular, the Commission has identified the following vulnerabilities in K Box's security arrangements which show how K Box failed to make reasonable security arrangements to protect the members' personal data:

(a) K Box could have, but failed to enforce its password policy, at least between 2 July 2014 and November 2014, thereby permitting the use of weak passwords:

(i) as noted at [9] above, K Box did not "conduct audit on whether the staff really use eight numbers/letters alphanumeric, one capital and one special case password [*sic*]"; and

(ii) even though it is a common industry practice to implement an organisation's password policy in its system, K Box had not done so earlier and the feature where the system would enforce the password policy by rejecting passwords that did not meet the password policy was only built into the CMS in November 2014.

(b) K Box had weak control over unused accounts, specifically, unused accounts were not removed:

(i) as stated at [14] above, as many as 36 accounts were removed from the CMS on 17 September 2014, which suggests that K Box may not have had the practice of deleting the accounts of staff that had left the company until it conducted the review on 17 September 2014. This is despite the fact that K Box was able to remove the unused accounts within a day after the List had been disclosed online which shows that K Box

could have easily removed the unused CMS accounts earlier but it had failed to do so;

(ii) as a result of K Box and/or Finantech's failure to promptly remove unused accounts from the CMS, the unused administrative CMS account with the user name "admin" and a weak password of "admin" remained in the CMS for about one year after Mrs G had left Finantech. This had put the personal data of K Box's members at risk because as noted at [20] above, Finantech itself had hypothesised that someone could have hacked into K Box's CMS using this "admin" user account and planted a malware control and command centre to retrieve and export the members' data; and

(iii) further, as noted at [18] above, there was evidence of multiple unauthorised accesses to the CMS through this "admin" user account in 2013 and between 25 February 2014 and 16 September 2014. As such, it is possible that K Box members' personal data could have been further compromised through this "admin" user account between 2 July 2014 and 16 September 2014 as a result of the failure to remove the unused administrative account.

(c) K Box failed to utilise newer versions of the software library and/or to conduct audits of the security of its database and system:

(i) K Box's CMS utilised an older version of the FCKEditor which according to security vulnerability website CVE, had at least nine known vulnerabilities which would have allowed cyber-attackers to install remote shells and execute malicious codes and to execute such codes to extract the full member list from the database. Even though this vulnerability could have been prevented by utilising newer versions of the software library or by patching, Finantech, whose role was to manage the CMS, had failed to do either; and

(ii) K Box had also failed to conduct audits to supervise the security of its database and system. As noted at [10] above, Finantech admitted that it did not carry out any system monitoring in terms of IT security, security testing or regular IT security audits at the time of the breach and prior to 17 September 2014.

27 K Box's weak enforcement of their password policy and weak control of unused accounts and passwords alone could have enabled an attacker to gain access to substantial personal data simply through the CMS. Furthermore, K Box's use of vulnerable software could have allowed the attacker to gain access to the system beyond the CMS limitations and to perform direct access to all data from K Box's database and potentially misuse the personal data.

28 The vulnerabilities set out above demonstrate that K Box could have done more to protect the members' personal data that was in its possession or under its control. When viewed in totality, the Commission is of the view that K Box had failed to make reasonable security arrangements to protect the members' personal data because these vulnerabilities were preventable and were likely the main reasons for the data breach and subsequent disclosure of the List on 16 September 2014. In this regard, while K Box had outsourced the developing, hosting and managing of its CMS to Finantech, it was still the data controller and was ultimately responsible for the security of the CMS.

29 Apart from the system-related shortcomings highlighted above, investigations disclosed that there were also poor practises.

(a) E-mails containing large volumes of personal data were sent via Gmail without any password-protection or encryption:

(i) Even though the unauthorised access to the personal data of about "317,000" K Box members was not caused by a breach that was the result of the use of unencrypted e-mails, as noted at [7] above, Finantech had previously sent K Box over 90,000 members' personal data via unencrypted e-mail via Gmail. The practice of sending large volumes of members' personal data via unencrypted e-mail is a vulnerability and an example of how K Box had not sufficiently protected the members' personal data. The better practice would have been for Finantech to encrypt or to ensure that the MS Excel document containing the list of members' personal data was password protected before sending it to K Box.[4]

4 See para 14.3 of the Personal Data Protection Commission's Guide to Securing Personal Data in Electronic Medium issued on 8 May 2015.

(b) K Box failed to effectively manage its vendor (Finantech) to ensure that it undertook adequate measures to protect members' personal data:

(i) For the reasons stated at [33] and [34] below, the Commission finds that Finantech is a data intermediary of K Box and pursuant to s 4(3) of the PDPA, K Box has the same obligations in respect of the personal data processed on its behalf and for its purpose by Finantech as if the personal data were processed by K Box itself. As highlighted in the Commission's Advisory Guidelines on Key Concepts in the Personal Data Protection Act issued on 23 September 2013 (at para 6.21) that:

> … it is very *important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in their written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question* including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation. [emphasis added]

(ii) However, as noted at [12] above, K Box failed to ensure that its data intermediary, Finantech, complied with a standard of protection in relation to the personal data transferred to it that is at least comparable to industry standards through its agreements and in its interactions with Finantech.

30 On the facts of the case and the assessment conducted, the Commission finds that both K Box and Finantech did not put in place adequate IT security arrangements between 2 July 2014 and November 2014, prior to the implementation of the new CMS in November 2014.

Issue B: Whether K Box had breached the Openness Obligation

31 Sections 11 and 12 of the PDPA together constitute the Openness Obligation under the PDPA, which provides that an organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. In particular, s 11(3) of the PDPA provides that an organisation shall designate one or more individuals, a DPO, to be responsible for ensuring that the organisation complies with the PDPA. In the same vein, s 12(*a*) of the PDPA requires organisations to

develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisations under the PDPA.

32 Based on investigations and representations made by K Box, the Commission is not satisfied that K Box has complied with the Openness Obligation under ss 11(3) and 12(*a*) of the PDPA. To begin with, as noted at [11] above, K Box conceded in its representations that it did not have a comprehensive privacy policy prior to 16 September 2014. By K Box's own admission, as there was no policy and physical or online security system in place to monitor whether a staff removed personal data from its premises, a K Box staff could have simply copied the members list it received from Finantech and abused that list. In addition, K Box had also represented that it did not have a DPO. In fact, to date, it is unclear whether K Box has appointed a DPO because Mr C represented that K Box was in the midst of appointing a DPO even as late as 20 April 2015 when he gave his statement to the Commission. In light of the foregoing lapses, the Commission finds that K Box has been in breach of the Openness Obligation.

Issue C: Whether Finantech is a data intermediary of K Box

33 Under s 2(1) of the PDPA, a "data intermediary" is an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation. The term "processing" in relation to personal data means the carrying out of any operation or set of operations in relation to the personal data and includes, but is not limited to, any of the following: recording; holding; organisation, adaptation or alteration; retrieval; combination; transmission; erasure or destruction.[5] Section 4(2) of the PDPA confers on a data intermediary the obligation to protect personal data under s 24 of the PDPA and the obligation to cease to retain personal data under s 25 of the PDPA. Save for the aforementioned obligations, Pts III to VI of the PDPA do not impose any other obligations on the data intermediary.

34 Having considered the facts and the representations made by K Box and Finantech, the Commission is satisfied that Finantech is a data intermediary of K Box. The fact that (a) K Box employees, including K Box's IT manager and the Chief Operating Officer, only had restricted

5 See s 2(1) of the Personal Data Protection Act (Act 26 of 2012).

access to the information of members, and (b) K Box relied on Mr G to extract and send them members' personal data with selected criteria from the database clearly shows that in practice, Finantech processed (by having access to, storing and retrieving) all personal data of K Box's customers pursuant to the arrangement between Finantech and K Box.

35 Notwithstanding that the "contracts", which were in fact quotations sent by Finantech to K Box for their confirmation and acceptance, pre-date the commencement of the data protection provisions of the PDPA and do not identify Finantech as a data intermediary of K Box, in light of the above practices which continued after the commencement of the data protection provisions, the Commission finds that Finantech is a data intermediary of K Box for the purposes of the PDPA.

Issue D: Whether Finantech had breached the Protection Obligation

36 Section 24 read with s 4(2) of the PDPA confers an obligation on the data intermediary to "[make] reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". In view of the Commission's finding that Finantech is a data intermediary of K Box, Finantech is required to comply with the obligation under s 24 of the PDPA to protect the personal data that it was processing on behalf of K Box.

37 In this regard, on the facts and circumstances, the Commission is of the view that Finantech had failed to put in place the required security measures that K Box needed in order to provide adequate protection for the personal data in K Box's database and system. In particular, the Commission notes that Finantech had been involved in the setting up and day-to-day processing of K Box's personal databases from 2007. By dint of its role and function, Finantech is expected to uphold a certain basic professional standard and the vulnerabilities identified at [26] to [29] above show that Finantech had not undertaken due diligence in executing its role. Finantech's failures had led to multiple unauthorised accesses and Finantech had put the personal data of K Box's members at risk.

38 If Finantech had advised K Box on its obligations but K Box had rejected their advice, the Commission could have taken this into account in its assessment of Finantech's culpability. However, investigations did not disclose any evidence to suggest that Finantech had actually advised K Box

of the need to have in place adequate security measures to protect the personal data in K Box's database. In fact, as stated at [12] above, Mr G admitted that he was only aware of the existence of the PDPA but not the specifics.

39 In view of all the relevant facts and circumstances, the Commission is not satisfied that Finantech has complied with the Protection Obligation under s 24 of the PDPA.

COMMISSION'S DIRECTIONS

40 Under s 29(1) of the PDPA, the Commission may, "if it is satisfied that an organisation is not complying with any provision in Parts III to VI of the Act, give the organisation such directions as the Commission thinks fit in the circumstances to ensure compliance with that provision". Section 29(2) of the PDPA also empowers the Commission to make all or any of the following directions:

(*a*) to stop collecting, using or disclosing personal data in contravention of this Act;

(*b*) to destroy personal data collected in contravention of this Act;

(*c*) to comply with any direction of the Commission under section 28(2); and

(*d*) to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

Other factors considered

41 In assessing the breach and the remedial directions to be imposed, the Commission took into consideration various factors relating to the case, including the mitigating and aggravating factors set out below.

K Box's breach of the Protection Obligation and the Openness Obligation

42 In relation to K Box's breach of the Protection Obligation and the Openness Obligation, the Commission took into account the following factors:

(a) the remedial actions undertaken by K Box were fair and prompt when they discovered the data breach in September 2014;

(b) most of the remedial actions were taken either in September or November 2014;

(c) the Commission found no evidence to suggest that the data breach was due to actions taken by K Box staff, through the CMS;

(d) a fairly large amount of personal data (of approximately "317,000" K Box members or more) had been disclosed as a result of the lack of security. The personal data comprising their full names, contact numbers, e-mail addresses, residential addresses, contact numbers, gender, profession, dates of birth and member numbers were sensitive data because it could have led to identify theft;

(e) K Box (as the primary data owner) had disregarded its obligations under the PDPA. K Box had ample opportunities to put in place reasonable security measures from 2 January 2013 to 2 July 2014 but it did not do so. K Box had also failed to appoint a DPO or put in place privacy policies or practices as late as April 2015. K Box had also failed to put in place data protection terms and conditions in its contract with Finantech, and instruct it (as the main data processor of K Box members' personal data) to protect personal data; and

(f) K Box was not forthcoming in providing information during the investigation. They had only provided bare facts in their responses during the investigations, which did not facilitate the Commission's investigations.

Finantech's breach of the Protection Obligation

43 In relation to Finantech's breach of the Protection Obligation, the following factors were taken into consideration:

(a) the remedial actions undertaken by Finantech were fair and prompt when they discovered the data breach in September 2014;

(b) most of the remedial actions were taken either in September or November 2014;

(c) a fairly large amount of personal data (of approximately "317,000" K Box members or more) had been put at risk as a result of the lack of security. The personal data comprising their full names, contact numbers, e-mail addresses, residential addresses, contact numbers, gender, profession, dates of birth and member numbers were sensitive data because it could have led to identify theft;

(d) Finantech as the data intermediary had disregarded its obligations under the PDPA. Finantech had ample opportunities to put in place reasonable security measures from 2 January 2013 to 2 July 2014 but it did not. There was no evidence to show that Finantech had advised K Box on the reasonable security measures that the owner of an online system ought to implement in order to protect personal data held by the system; and

(e) Finantech appeared not to be forthcoming in providing information during the investigation. Although the Notices to Require Production of Documents and Information under the Ninth Schedule to the PDPA ("NTPs") were sent to Finantech as early as October 2014, Finantech's responses to these NTPs were only provided in April 2015 – almost seven months after the NTPs were first issued. This delayed the investigation process.

44 Having completed its investigation and assessment of this matter, the Commission is satisfied that K Box has been in breach of the Protection Obligation under s 24 of the PDPA and the Openness Obligation under ss 11(3) and 12(*a*) of the PDPA for the reasons cited at [26] to [28] and [31] above. Pursuant to s 29(2) of the PDPA, the Commission hereby directs K Box to do as follows:

(a) pay a financial penalty of $50,000 within 30 days from the date of the Commission's direction, failing which interest at the rate specified in the Rules of Court[6] in respect of judgment debts shall be payable on the outstanding amount of such financial penalty; and

(b) appoint a DPO within 30 days from the date of the Commission's direction (if it has not already done so).

45 The Commission is also satisfied that Finantech has not complied with the Protection Obligation under s 24 of the Act for the reasons cited at [33], [34], [36] and [37] above. Pursuant to s 29(2) of the PDPA, the Commission hereby directs Finantech to do as follows:

Pay a financial penalty of $10,000 within 30 days from the date of the Commission's direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall be payable on the outstanding amount of such financial penalty.

---

6 Cap 322, R 5, 2014 Rev Ed.

46 The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA and with the Commission's directions.

LEONG KENG THAI
Chairman
Personal Data Protection Commission

Grounds of Decision

Re The Institution of Engineers Singapore

Case Number: DP-1411-A213
Decision Citation: [2016] SGPDPC 2

Protection Obligation *– Access to personal data – Insufficient technical security arrangements*

20 April 2016

BACKGROUND

1 The Institution of Engineers Singapore (UEN S66SS0041B) ("IES") is a society registered with the Registry of Societies. IES was formally established on July 1966 as the national society of engineers in Singapore. Its functions include the accreditation of engineering academic programmes (through its Engineering Accreditation Board); the maintenance of professional registries; and the promotion of social, business, professional and career development amongst engineers in Singapore.

The IES website

2 IES operates a website at <www.ies.org.sg> ("Site"), which consists of both publicly-accessible pages, and a members' portal, accessible only by members of IES, upon logging into the portal with their respective user identifications ("IDs") and passwords. The Site also allows members of the public, who are non-IES members, to create an account on the Site in order to login to access and post on the Site's forums.

3 According to information provided by IES, the functions of the Site include:

(a) enabling members to update their membership details such as addresses, e-mails and contact information;
(b) applying for courses and events that are created by IES;
(c) applying for e-mail addresses with ies.org.sg domain, *eg*, abc@ies.org.sg;

(d) payment for membership and courses via PayPal;
(e) accessing webmail;
(f) allowing members to search for information about other members;
(g) publishing information on IES events, courses, seminars, job listings, and information on various registries (*eg*, ABC Waters Professional Registry and others);
(h) applying for IES membership; and
(i) accessing IES forums.

4 Members of IES who log in to the Site using their membership user IDs are able to access certain dedicated membership Site functions, including receipt of *ad hoc* AGM notices, quick poll functions, profile updates and change of passwords.

Data Leak incident

5 On 1 October 2014, the Personal Data Protection Commission ("Commission") was informed that the information of users of the Site had been posted on <http://pastebin.com> ("Pastebin"), a website which allows members of the public to post and share information online ("Data Leak").

6 The relevant information was ostensibly uploaded onto the Pastebin website by a Pastebin user with the username "KAMI_HAXOR", in the form of two posts in plain text that could be publicly viewed by any visitor to the Pastebin website. The two posts were dated 30 September 2014 and were respectively captioned:

(a) "IES.ORG.SG 6,000+ Usersnames + pass Leaked by KaMi HaX" ("User ID List"); and
(b) "Ies.org.sg 60,000+ Users Data Leaked by KaMi HaXor" ("Additional List").

7 The User ID List was titled "The Institution of Engineers Singapore 6000= [*sic*.] users, 90,000+ Mobiles leaked By KaMi HaXor … Target= http://www.ies.org.sg/", and contained a list of characters separated with a colon, in the format "XXXX:XXXX", which was labelled "MemberId:Pass".

8 The Additional List was titled "*The Institution of Engineers Singapore 60,000+ Mobiles leaked By KaMi HaXor … Target= http://www.ies.org.sg/*", and contained a list of eight-digit numbers that were consistent with the format of Singapore telephone numbers.

9 In light of the information received, the Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether there had been a breach by IES of its obligations under the PDPA.

Nature of the Data Leak incident

10 IES informed the Commission that the passwords and IDs in the User ID List were those of IES members and that it was made aware of the Data Leak by one Nicholas Lee, who had written to IES on 1 October 2014 at 10.13am, to inform IES about the Data Leak.

11 IES also provided the Commission with a copy of a Site audit report which was conducted by its website vendor, Forecepts Pte Ltd ("Forecepts"), using Acunetix software, in the aftermath of the Data Leak. The report, titled "Acutenix Website Audit Developer Report", dated 3 November 2014 ("First Scan Report") indicated a number of vulnerabilities with the Site, including 48 high-severity vulnerabilities in the Site set out below:

High-Severity Type Vulnerability Identified	Variation
Blind SQL Injection	1
Cross site scripting	8
Cross site scripting (verified)	30
Cross site scripting [stored] (verified)	1
FCKeditor spellchecker.php cross site scripting vulnerability	2
HTML Form found in redirect page [high severity]	4
jQuery Cross Site Scripting	1
PHP allow_url_fopen enabled	1

12 Forecepts suspected that the attack on the Site was likely to have been caused by cross-site scripting but was unable to confirm this. In any case, the Commission notes that cross-site scripting was identified in the First Scan Report as a high-severity vulnerability that existed in the Site.

13 In relation to the number of individuals affected by the Data Leak, the Commission notes that the titles of the User ID List and the Additional

1 Act 26 of 2012.

List respectively indicate that the data of more than 6,000 users had been disclosed in the User ID List, and that the data of more than 60,000 users had been disclosed in the Additional List. However, IES submitted that it was unable to identify the total number of IES members who were affected by the Data Leak, as the "data published online are in random".

14 At the time of this decision, both the User ID List and the Additional List appear to have been removed from the Pastebin website.

15 Having reviewed the relevant facts and circumstances, including the written responses to the Notices to Require Production of Documents and Information under the Ninth Schedule to the PDPA ("NTPs") submitted by IES, the Commission sets out below its findings and assessment in relation to the Data Leak.

COMMISSION'S FINDINGS AND ASSESSMENT

Personal data leaked

16 "Personal data" is defined under s 2 of the Act, as follows:

> 'personal data' means data, whether true or not, about an individual who can be identified —
>
> (*a*) from that data; or
>
> (*b*) from that data and other information to which the organisation has or is likely to have access.

17 As noted above, IES admitted that the passwords and IDs in the User ID List belonged to its members. According to publicly-available information on the Site, IES's membership comprises both individuals and organisations. Organisation members may be represented in IES by up to two individuals from the organisation. Individuals who are not part of any organisation can also join as members of IES with the relevant engineering qualifications.

18 IES also acknowledged that the personal data of its members were stored on its web server and could be retrieved using the members' respective user IDs and passwords. In particular, IES stated that "personal data such as Member ID, Name, Contact, Email and Address were stored in the database in www.ies.org.sg".

19 In light of the foregoing, it is clear that the person or persons who had obtained and posted the User ID List on the Pastebin website in the first place, as well as any member of the public who came across the User ID List on the Pastebin website, could have used the IDs and passwords disclosed to log in to the accounts of individual and organisation members (represented by their nominated employees) on the Site, and thereby access personal data relating to these members that were stored on the Site.

20 Furthermore, given that anyone who had obtained a valid user ID and password combination would have been able to log in to the Site to retrieve personal details relating to the respective IES member, the Commission is of the view that anyone with a valid user ID and password combination would effectively be able to access the entire profile of an IES member and identify him. Accordingly, the Commission is of the view that the user IDs and passwords that were leaked would fall within the definition of "personal data" under the PDPA.

21 The Commission notes that IES had taken the view that the possibility of any individual using the information in the User ID List to access the personal data in IES's webserver was remote as the listing of user IDs and passwords was "random, unrelated and unlinked". IES was also of the view that it was unlikely that the person or persons who had obtained and posted the User ID List on the Pastebin website had used the IDs and passwords displayed to log in to the accounts of its members on the Site to access personal data stored on the Site "or he would have placed the relevant information in a different (database) format" [*sic*].

22 The Commission disagrees with the views expressed by IES. The risk of access by any individual using the user IDs and passwords combination in the User ID List is not remote. The User ID list is effectively a dictionary of valid user IDs and passwords that can be used in a dictionary attack. With automatic scripting, an individual can log in to any IES member's account notwithstanding that the manner in which the user IDs and passwords had been presented in the list appeared "random, unrelated and unlinked". Indeed, the Commission cannot exclude the possibility that the person or persons who had obtained and posted the User ID List on the Pastebin website may have already done so notwithstanding the lack of complaints of abuse of personal data from IES members thus far.

23 Accordingly, it is clear that, as a result of the Data Leak, the security of personal data relating to IES members was compromised as such personal

data could have been accessed by one or more unauthorised persons with knowledge of the leaked user IDs and passwords.

Personal data under the possession and control of IES

24 The Commission notes that, at all material times, the Site was fully owned and administered by IES. For completeness, the Commission also notes that although IES had engaged two vendors for the Site, these vendors undertook their respective functions on behalf of IES and did not own or administer the Site:

(a) Forecepts, as IES's website vendor, was engaged to supply and design the website design and content management system. Forecepts was also engaged to provide maintenance to the Site, but only upon request by IES; and

(b) the Site was hosted at the premises of ReadySpace (SG) Pte Ltd ("ReadySpace"), IES's hosting service provider, on a dedicated server.

25 Further, the Commission's investigations found that there were four individuals within IES who could access the list of member IDs and passwords and personal data relating to IES members. These were IES's information technology ("IT") manager, IT executive, membership manager and membership executive.

26 Accordingly, the Commission is satisfied that, at all material times, the relevant personal data of IES members, which were stored on the Site and whose security was compromised as a result of the Data Leak, were in the possession and/or under the control of IES.

Adequacy of security arrangements

27 Section 24 of the PDPA states:

> **Protection of personal data**
> **24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

28 Pursuant to s 24 of the PDPA, IES, being an organisation which had its members' personal data under its possession and/or control, is required to make reasonable security arrangements to prevent unauthorised access,

collection, use, disclosure, copying, modification, disposal or similar risks ("Protection Obligation").

29 IES informed the Commission that it had put in place the following security measures at the material time:

(a) the Site's server was hosted on a secure site and on a dedicated server, and protected by a firewall and anti-virus software (namely, Parallels Plesk Panel 11.0.9);

(b) software updates had been performed on the Parallels Plesk Panel 11.0.9 firewall and anti-virus software; and

(c) a list of user IDs and passwords relating to the IES members could be extracted from the members' portal and saved; however, such a function could only be performed by the four individuals within IES who could access the list of member IDs and passwords (namely, IES's IT manager, IT executive, membership manager and member executive). Forecepts was also authorised to access such a function for the purposes of maintaining, troubleshooting and updating the Site.

30 However, from the Commission's investigations, it was also apparent that:

(a) the Site had not provided for the encrypted storage of member passwords;

(b) prior to the Data Leak, no audit had been conducted on ReadySpace's enterprise hosting services and/or the security of the Site;

(c) IES had not conducted any penetration testing on the Site, and was not aware of penetration testing software; and

(d) while IES represented that it had made phone calls to its vendors ReadySpace and Forecepts to inform them about the PDPA, there was no indication that IES had otherwise given instructions to its vendors to make security arrangements so as to ensure that personal data stored on the Site would be protected in compliance with IES's obligations under the PDPA. Furthermore, the contractual terms between IES and its vendors, as submitted by IES, did not appear to contain any specific security arrangements or requirements for its vendors to put in place security measures to safeguard IES members' personal data stored on the Site.

31 In addition, as already mentioned earlier, the First Scan Report by Forecepts following the Data Leak indicated that there existed a number of

vulnerabilities within the Site, including 48 high-severity vulnerabilities such as cross-site scripting and SQL injections.

32 Cross-site scripting is a common web vulnerability, which could have been easily detected by performing a vulnerability scan, such as the one performed by Forecepts after the Data Leak. Once identified, the vulnerabilities can be patched according to the many guides that are readily available on the Internet. The conduct of vulnerability scans using automated tools like Acunetix is considered industry best practice.

33 In this case, IES acknowledged that it had not undertaken any sort of audit to detect security vulnerabilities in the Site. IES had also not demonstrated that it had made any effort to require its vendors to evaluate and/or ensure the security of personal data stored on the Site.

34 While the Site may have had a firewall and anti-virus software in place, these measures alone were clearly inadequate to reasonably ensure the security of personal data stored on the Site, as the firewall and anti-virus software would not protect against common vulnerabilities such as cross-site scripting. This would have been apparent, and indeed was made apparent, by a vulnerability scan such as the one conducted by Forecepts after the Data Leak.

35 From the above, it would appear that prior to the Data Leak, IES had made insufficient effort to inquire into and/or ensure the security of personal data stored on the Site. As a result, numerous security vulnerabilities existed in the Site at the time of the Data Leak, which could have been reasonably detected and patched by available means.

36 In light of the foregoing, the Commission is of the view that IES has failed to make reasonable security arrangements in respect of personal data relating to its members, as required under the Protection Obligation.

COMMISSION'S DIRECTIONS

37 In its representations to the Commission, IES took the position that it was a small organisation that had relied on external specialists for security related advice and hence should not be heavily penalised for any breaches of the data protection provisions. IES was of the view that its external specialists had not advised any actions on possible areas of protection and/or detection until the breach to the Site occurred.

38 However, the Commission notes that IES' claims regarding its reliance on external specialists were not borne out by the investigations. Further, IES, as an organisation with several thousand members, cannot be described as "a small organisation".

39 In determining the directions to be given to IES, the Commission has given due consideration to all the relevant factors, including the following:

(a) IES was co-operative and forthcoming throughout the Commission's investigation;

(b) following its discovery of the Data Leak on 1 October 2014, IES promptly took the following measures to manage the effects of the Data Leak:

(i) disabling of the members' portal on the Site;

(ii) changing of the passwords for all IES members' accounts, and resetting of the passwords for its administrator accounts in the members' portal;

(iii) on 2 October 2014, IES sent an e-mail notification to all IES members, informing them of the "hacking activity" on the Site, as well as the measures (listed in (i) and (ii) above) IES had taken to minimise damage; and

(iv) removal of the telephone numbers and addresses of IES members previously stored on the database of the Site;

(c) following the Data Leak, IES implemented the following additional security measures:

(i) instructed Forecepts to conduct a security audit of the Site and to patch up any vulnerabilities detected pursuant to such audit, and to conduct a monthly audit on the Site upon completion of the security hardening process;

(ii) installation of a new intrusion detection system, along with endpoint protection in the Site's server; and

(iii) installation of Secure Sockets Layer ("SSL") certification in the Site's server; and

(d) the high-severity vulnerabilities identified in the First Scan Report pursuant to Forecepts' audit of the Site appear, from the Acunetix Website Audit Developer Report dated 12 January 2015, which was provided by IES to the Commission ("Second Scan Report"), to have been patched by Forecepts.

40 Pursuant to s 29(2), and having completed its investigations and assessment of this matter, the Commission is satisfied that IES was in breach of the Protection Obligation under s 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commission hereby directs IES to do the following:

(a) IES shall within 60 days from the date of the Commission's direction:

(i) conduct a further vulnerability scan of the Site; and

(ii) patch all vulnerabilities identified by such scan;

(b) IES shall, in addition, submit to the Commission by no later than 14 days after the conduct of the abovementioned vulnerability scan, a written update providing details on:

(i) the results of the vulnerability scan; and

(ii) the measures that were taken by IES to patch all vulnerabilities identified by the vulnerability scan; and

(c) IES shall pay a financial penalty of $10,000 within 30 days from the date of the Commission's direction, failing which interest shall be payable on the outstanding amount of such financial penalty.

41 The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA and with the Commission's directions.

LEONG KENG THAI
Chairman
Personal Data Protection Commission

Grounds of Decision

Re Fei Fah Medical Manufacturing Pte Ltd

Case Number: DP-1409-A145
Decision Citation: [2016] SGPDPC 3

Protection Obligation *– Access to personal data – Insufficient technical security arrangements*

20 April 2016

BACKGROUND

1 Fei Fah Medical Manufacturing Pte Ltd (UEN 199800455H) ("Fei Fah Medical") is a locally registered company specialising in the development and manufacture of healthcare and beauty products.

The Ripple website

2 Fei Fah Medical operates a website under the name Ripple Tea Company at <www.ripple.com.sg> ("Site").

3 The Site consists of both publicly accessible pages, and a members' portal (which is accessible only by individuals who had signed up with Fei Fah Medical under a membership scheme called Ripple Club, upon logging into the portal with their respective user identifications ("IDs") and passwords).

Data leak incident

4 On 29 September 2014, the Personal Data Protection Commission ("Commission") was informed that information of users of the Site had been posted on <http://pastebin.com> ("Pastebin"), a website which allows members of the public to post and share text online publicly ("Data Leak").

5 The relevant information was ostensibly uploaded onto the Pastebin website by a Pastebin user with the username "KAMI_HAXOR", in the

form of a post in plain text that could be publicly viewed by any visitor to the Pastebin website.

6 The post was undated and captioned: "Ripple Tea Company Singapore 900+ Users emails+passes+Names+mobile Numbers With Subscribers Emails Leaked By KaMi HaXor".

7 The post contained a list of data, which were numbered from 1 to 2,981, ostensibly to indicate that there were 2,981 entries in it. The data in the post appeared to have been sorted into the following three categories:

(a) e-mail addresses – there were 1,114 entries of e-mail addresses, the e-mail addresses were unaccompanied by other data or identifiers and 219 of the entries contained "*.sg*" domain names;

(b) user IDs and encrypted passwords to Ripple Club accounts – there were 876 entries of user IDs and passwords, which had been encrypted using an MD5 message-digest algorithm, a commonly used cryptographic hash function producing a 128-bit (16-byte) hash value; and

(c) telephone numbers – there were 836 entries of telephone numbers containing between seven and ten digits. It was unclear whether the telephone numbers were Singapore or Hong Kong telephone numbers as the format of telephone numbers used by the countries is similar.

8 In light of the information received, the Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether there had been a breach by Fei Fah Medical of its obligations under the PDPA.

Nature of the Data Leak incident

9 In its responses to the Commission, Fei Fah Medical confirmed that the data in the list were those of prospective customers and general enquirers to its Ripple brand products.

10 Fei Fah Medical further confirmed that the data were collected via its Site and stored in a database based in Hong Kong. Fei Fah Medical had

1 Act 26 of 2012.

outsourced all its web development and hosting functions to its Hong Kong-based data intermediary, IT Factory. IT Factory had in turn engaged HKNet Company Limited, also based in Hong Kong, to provide the actual hosting services for the database.

11 Fei Fah Medical indicated that it had no knowledge of the Data Leak prior to receiving the Commission's Notice dated 1 October 2014. However, after being alerted to the Data Leak, it sent e-mail notifications to all affected individuals, informing them that there had been hacking activity on the Site and that their personal data may have been compromised.

12 Fei Fah Medical also took steps to instruct IT Factory to remove all data collecting functions from its Site. However, as these instructions failed to be carried out by IT Factory, new data continued to be collected via the Site till 30 July 2015 (almost ten months after Fei Fah Medical was first notified about the Data Leak), when the Commission alerted Fei Fah Medical to the fact that the Site still retained its data collecting functions.

13 Fei Fah Medical was unable to ascertain how the Data Leak could have occurred and did not appear to be familiar with the security measures which were used on the Site at the material time. In fact, in its responses to the Commission, Fei Fah Medical simply stated the cause of the Data Leak to be "unknown" and was unable to provide any logs or files capturing the intrusion to its data system.

14 Fei Fah Medical also appeared to be uncertain about which individuals or organisations had access to the leaked data. Although Fei Fah Medical initially stated that the leaked data were only accessible by "the actual host", HKNet Company Limited, it later clarified that the data were also accessible at the material time by its own backend administration staff (*ie*, those who administered the database), and by using the staff ID of one of its directors, [redacted] ("Mr L"). Additionally, it admitted that it would have been possible for a hacker to access the database to extract the data by seeding "some program in the server".

15 Overall, Fei Fah Medical was unable to explain how the Data Leak occurred. It was also unable to explain or provide sufficient information on the security measures implemented on either the Site or database at the material time.

16 In relation to the number of individuals affected by the Data Leak, the Commission notes that the title of the post indicates that the data of

approximately 900 users had been disclosed in the data list. Although Fei Fah Medical claimed that not all the information in the data list was accurate, it did not dispute the number of users who were affected by the Data Leak.

17 Having reviewed the relevant facts and circumstances, including the written responses to the Notices to Require Production of Documents and Information under the Ninth Schedule to the PDPA ("NTPs") submitted by Fei Fah Medical, the Commission sets out below its findings and assessment in relation to the Data Leak.

COMMISSION'S FINDINGS AND ASSESSMENT

Personal data leaked

18 As noted above, there were three categories of data found in the post on the Pastebin website. Fei Fah Medical acknowledged in its representations to the Commission that the data in the post were those of prospective customers and general enquirers to its Ripple brand products. Fei Fah Medical also acknowledged that personal data of Ripple Club members were stored in its database, which could be retrieved with the appropriate user ID and password.

19 Although the passwords were encoded, they had been encoded using an MD5 message-digest algorithm, a commonly used cryptographic hash function, which could be easily attacked with password tables by any motivated individual.

20 Further, given that anyone who had obtained a valid user ID and password combination would be able to log in to the Site to retrieve personal details relating to the respective Ripple Club member, it is apparent that a valid user ID and password combination would be able to identify an individual Ripple Club member. Accordingly, the Commission is of the view that the user IDs and passwords that were leaked would fall within the definition of "personal data" in the Act.[2]

21 In addition, several of the telephone numbers disclosed in the data list appeared to be personal mobile telephone numbers, which would, by

2 Personal Data Protection Act 2012 (Act 26 of 2012) s 2.

themselves, be able to lead to the identification of the individuals owning the numbers. Similarly, several of the e-mail addresses display, what seems to be, the full names of the respective owners of the e-mail addresses, and appear capable of identifying them. Those telephone numbers and e-mail addresses thereby constitute "personal data" under the Act.[3]

Personal data under the possession and control of Fei Fah Medical

22 Fei Fah Medical confirmed the fact that the Site was fully owned and administered by it at all material times. The personal data of Fei Fah Medical's Singaporean users were also generally collected via the Site from Singapore.

23 For completeness, the Commission notes Fei Fah Medical's statements that:

> (a) IT Factory, as Fei Fah Medical's website vendor, was engaged to supply and design the website and to provide maintenance upon request; and
> (b) the contents collected via the Site were stored in a database hosted at the premises of HKNet Company Limited, a data hosting service provider, on a dedicated server.

24 It is apparent from the information provided by Fei Fah Medical that IT Factory and HKNet Company Limited, as Fei Fah Medical's vendors, undertook these functions on behalf of Fei Fah Medical.

25 Although Fei Fah Medical initially stated that the leaked data were only accessible by HKNet Company Limited, it subsequently clarified that the data were also accessible at the material time by its backend administration staff (*ie*, those who administered the database), and by one of its directors, Mr L. In fact, Fei Fah Medical remained in control of the personal data stored in the database hosted by HKNet Company Limited at all material times, as evidenced by Fei Fah Medical's instructions to IT Factory to delete all the personal data subsequent to the Data Leak.

26 Accordingly, the Commission is satisfied that, at all material times, the relevant personal data of users of the Site and whose security was

---

3 Personal Data Protection Act 2012 (Act 26 of 2012) s 2.

compromised as a result of the Data Leak, were in the possession and/or under the control of Fei Fah Medical.

Adequacy of security arrangements

27 Fei Fah Medical, being an organisation which had its Site users' personal data under its possession and/or control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks ("Protection Obligation").[4]

28 However, Fei Fah Medical was unable to provide any information about the security arrangements that it had put in place to protect either the Site or the server where the database of personal data collected was hosted.

29 Although Fei Fah Medical claimed that it had set up some firewalls within the administration control panel, it was neither able to provide details as to the nature of these firewalls nor any evidence as to their existence in its responses to the NTPs issued by the Commission.

30 In the Commission's view, the facts demonstrate that, prior to the Data Leak, Fei Fah Medical had made little effort to inquire into and/or ensure the security of personal data stored on the Site. Fei Fah Medical appeared to have little knowledge as to whether there were security measures implemented on its Site or the server where the database of personal data collected was hosted.

31 In light of the foregoing, the Commission is of the view that Fei Fah Medical has failed to make reasonable security arrangements in respect of personal data relating to users of its Site, as required under the Protection Obligation.

COMMISSION'S DIRECTIONS

32 At the time of this decision, the list of data appears to have been removed from the Pastebin website.

---

4 Personal Data Protection Act 2012 (Act 26 of 2012) s 24.

33 In determining the directions to be given to Fei Fah Medical, the Commission has given due consideration to all the relevant factors, including the following:

(a) Fei Fah Medical had been neither co-operative nor forthcoming in its responses to the NTPs issued by the Commission as part of its investigations. In this regard, the Commission notes that Fei Fah Medical had provided incomplete responses to the first and second NTPs issued by the Commission, and initially ignored the third NTP issued by the Commission. Fei Fah Medical also took between three weeks to a month to respond to each NTP and its responses were not forthcoming; and

(b) although Fei Fah Medical took steps to instruct its Hong Kong-based data intermediary IT Factory to implement remedial actions to address the Data Leak following its discovery on 1 October 2014, it did not ensure that its instructions were carried out by its data intermediary. The data intermediary only implemented remedial actions to address the Data Leak on 30 July 2015, more than ten months after Fei Fah Medical first discovered the Data Leak. This undue delay in implementing the remedial actions suggests a continuing insouciance by Fei Fah Medical with respect to its obligation to make reasonable security arrangements to keep personal data in its possession or under its control protected.

34 Pursuant to s 29(2), and having completed its investigation and assessment of this matter, the Commission is satisfied that Fei Fah Medical has been in breach of the Protection Obligation under s 24 of the PDPA.

35 The Commission notes from the representations submitted by Fei Fah Medical's lawyers on its behalf to the Commission that it intends to shut down the Site and replace it with a newly constructed website within four months. Having carefully considered all the relevant factors of this case, the Commission hereby directs Fei Fah Medical to do the following:

(a) Fei Fah Medical shall within 120 days from the date of the Commission's direction:

(i) implement a new website to replace the Site;

(ii) conduct a web application vulnerability scan of the new website; and

(iii) patch all vulnerabilities identified by such scan;

(b) Fei Fah Medical shall, in addition, submit to the Commission by no later than 14 days after patching all vulnerabilities identified by the abovementioned vulnerability scan, a written update providing details on:

(i) the results of the vulnerability scan; and

(ii) the measures that were taken by Fei Fah Medical to patch all vulnerabilities identified by the vulnerability scan; and

(c) Fei Fah Medical shall pay a financial penalty of $5,000 within 30 days from the date of the Commission's direction, failing which interest, at the rate specified in the Rules of Court[5] in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

36 The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA and with the Commission's directions.

LEONG KENG THAI
Chairman
Personal Data Protection Commission

5 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Universal Travel Corporation Pte Ltd

Case Number: DP-1508-A496
Decision Citation: [2016] SGPDPC 4

Consent Obligation *– Disclosure of personal data without consent*
Notification Obligation *– Disclosure of personal data without notification*
Openness Obligation *– Lack of data protection policies and practices*
Purpose Limitation Obligation *– Disclosure of personal data for purposes that a reasonable person would consider appropriate in the circumstances*

20 April 2016

BACKGROUND

1 The Personal Data Protection Commission ("Commission") received a complaint from a credible source concerning the alleged disclosure by the Respondent of personal data of 37 customers ("passenger list") in early March 2015 to certain individual(s) who participated in the 12 Days Legend of the Balkans Tour from 17 February 2015 to 28 February 2015 ("Balkans Tour").

2 In the premises, the Commission decided to carry out an investigation into the matter. The Commission's findings are set out below.

MATERIAL FACTS AND DOCUMENTS

3 Sometime in or around late February 2015, four of the customers of the Balkans Tour requested the Respondent to furnish formal documentation confirming the cancellation of their transit flight to Sofia on 18 February 2015 (TK1027/18FEB15 ISTANBUL-SOFIA) ("formal confirmation") to process their insurance claims.

4 The Respondent therefore requested from Turkish Airline written confirmation of the flight cancellation and the affected passenger list.

5 Sometime in early March 2015, the Respondent sent the formal confirmation together with the letter from Turkish Airline and the

passenger list by e-mail to four of the customers of the Balkans Tour. The passenger list that was sent contained the name, nationality, date of birth, passport number, passport expiry date and passenger name record (a record in the database of a computer reservation system ("CRS") that contains the itinerary for a passenger, or a group of passengers travelling together) of all 37 of the passengers/customers that were on the Balkans Tour. The passengers' details were not masked or redacted when it was sent by the Respondent. It is not disputed that the passengers' details constituted personal data under the control of the Respondent at the material time.

6 In the Respondent's response to the Commission during the investigation, the Respondent confirmed to the Commission that it did not obtain consent from the 37 passengers to disclose their personal data to other parties. It also mentioned that none of the passengers had authorised the release of their personal data to third parties. The Respondent confirmed to the Commission that it also did not have any personal data policy in place at the material time.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

7 The issues in this case to be determined are as follow:

(a) Has the Respondent complied with ss 13[1] and 20[2] of the Personal Data Protection Act 2012[3] ("PDPA") in disclosing the personal data to the customers of the Balkans Tour?

---

1 Section 13 of the Personal Data Protection Act 2012 (Act 26 of 2012) prohibits an organisation from collecting, using or disclosing an individual's personal data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data. This provision is also to be read with ss 14, 15 and 20 of the Act.

2 Section 20 of the Personal Data Protection Act 2012 (Act 26 of 2012) requires, amongst other things, that an organisation informs an individual of (a) the purposes for the collection, use or disclosure of personal data, on or before collecting the personal data; and (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under para (a) above before the use or disclosure of the personal data for that purpose.

3 Act 26 of 2012.

(b) Was the disclosure of the personal data made in accordance with s 18 of the PDPA,[4] *ie*, for purposes that a reasonable person would consider appropriate in the circumstances?

(c) Has the Respondent complied with s 12(*a*) of the PDPA[5] in developing and implementing policies and practices necessary to meet its obligations under the PDPA?

Contraventions by the Respondent under sections 13 and 20 of the PDPA

8 The Commission notes that the Respondent intentionally sent the passenger list to the four individuals who had requested for confirmation of the flight cancellation.

9 However, the Respondent had not sought for or obtained any of the 37 passengers' consent in disclosing their information contained in the passenger list to the other individual(s) who were requesting for the formal confirmation from the Respondent. In this regard, the Respondent did not have the requisite consent from the 37 passengers to disclose their personal data to the other individual(s) under s 14 of the PDPA.

10 In relation to whether the 37 passengers could be deemed to have consented to the disclosure of the personal data under s 15 of the PDPA, the Commission finds that no such deemed consent can be imputed on the facts. The Commission notes that when the 37 passengers voluntarily provided their personal data to the Respondent, the purposes for providing their personal data did not include the purpose of allowing another passenger to process his insurance claim. This is fortified by the Respondent's confirmation that none of the passengers had agreed or authorised the release of their personal data to a third party. The

4 Section 18 of the Personal Data Protection Act 2012 (Act 26 of 2012) provides that an organisation may collect, use or disclose personal data about an individual only for purposes (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under s 20, if applicable.

5 Section 12(*a*) of the Personal Data Protection Act 2012 (Act 26 of 2012) provides that an organisation shall develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation.

Commission notes that each individual only required his flight details and confirmation of the flight delay in order to process his insurance claim.

11 In its submissions to the Commission, the Respondent claimed that the exception provided for in para 1(*a*) of the Fourth Schedule to the PDPA ("exception") applied[6] to the case and hence it was not required to seek the consent of the individuals concerned for the disclosure of the 37 passengers' personal data.

12 Having considered the context and circumstances of the case, the Commission concludes that the aforesaid exception does not apply for the following reasons:

(a) "Interests of the individual" under para 1(*a*) of the Fourth Schedule should refer to the interests of the data subject. Disclosing the personal data of other passengers to a fellow passenger for the purpose of enabling that passenger to make a claim against his travel insurance policy for himself cannot be said to be in the interest of any one or all of the other passengers.

(b) It does not appear obvious to the Commission that in order to make an insurance claim, details of all other affected passengers on the Balkans Tour had to be disclosed. For one, the Respondent could have provided the confirmation with only the details of the individual making the insurance claim. Alternatively, the other passengers' details could be removed or redacted in the list when it was forwarded to the recipients. There is no suggestion otherwise that these actions could not be carried out.

(c) There is nothing to suggest that consent for disclosure could not be secured from the passengers in the list in a timely manner, or that there was urgency in the matter which warranted the consent from the other passengers to be dispensed with.

---

6 Paragraph 1(a) of the Fourth Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012) states that an organisation may disclose personal data about an individual without the consent of the individual if the disclosure is necessary for any purpose which is clearly in the interests of the individual and if consent for its disclosure cannot be obtained in a timely way.

13 In the circumstances, by disclosing the passenger list containing the personal data of the 37 passengers without obtaining their prior consent, the Respondent had contravened s 13 of the PDPA. Additionally, since the Respondent had also not informed them of the purposes for which it was disclosing their personal data, it is also in breach of s 20 of the PDPA.

Disclosure of personal data was not for purposes reasonable or appropriate in the circumstances or for purposes that the individual has been informed of under section 20

14 In view that the disclosure of the entire passenger list goes beyond supporting an individual customer's insurance claim (as set out at [12(a)] and [12(b)] above), the disclosure could not be for purposes that a reasonable person would consider appropriate in the circumstances.

15 In addition, since the Respondent had not been informed of the purposes for which it was disclosing the passengers' personal data, it was also not in compliance with s 20 of the PDPA.

16 In this regard, the Respondent was also in breach of s 18 of the PDPA.

Failure to develop and implement policies and practices necessary to meet obligations under the PDPA

17 Given that the Respondent had not put in place data protection policies to ensure compliance with the PDPA at the material time when the data breach transpired, as confirmed by the Respondent in its response to the Commission's request for information and documents on 13 August 2015, the Respondent was in breach of s 12(*a*) of the PDPA.

18 The Commission notes from the Respondent's response of 24 August 2015 that the Respondent is taking steps to set up guidelines with regard to the use and disclosure of customers' personal data to comply with s 12(*a*) of the PDPA.

ENFORCEMENT ACTION TAKEN BY THE COMMISSION

19 Given the Commission's findings that the Respondent is in breach of its obligations under ss 12(*a*), 13, 18 and 20 of the PDPA, the Commission is empowered under s 29 of the PDPA to give the Respondent 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 $1m as the Commission thinks fit.

20 In exercise of the power conferred upon the Commission pursuant to s 29 of the PDPA, the Commission directs the Respondent to take the following steps:

(a) to put in place within three months a data protection policy and internal guidelines to comply with the provisions of the PDPA and, in particular, to prevent future recurrences of the breaches that had occurred in this matter;

(b) to inform within two weeks the individuals who received the passenger list not to disclose the list to other third parties;

(c) for all employees of the Respondent handling personal data to attend a training course on the obligations under the PDPA and the organisation's data protection policies within six months from the date of this decision; and

(d) to inform the Commission of the completion of each of the above within one week.

21 On a balance, the Commission has decided not to impose a financial penalty on the Respondent in view of the overall circumstances of the matter, namely:

(a) that the disclosures were made to a limited number of persons and to their personal e-mail addresses;

(b) that the personal data that were disclosed were in relation to limited individuals;

(c) that the disclosures were not due to a systemic issue that could result in further disclosures being made or further harm being caused;

(d) that the disclosures appear to be caused by the lack of awareness on the Respondent's employees' part of data protection obligations; and

(e) that the disclosures were *bona fide* mistakes made by the Respondent's employees who were seeking to assist the passengers with their insurance claims, and not one where there was a wilful disregard for the provisions in the PDPA.

22 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re YesTuition Agency

Case Number: DP-1407-A028
Decision Citation: [2016] SGPDPC 5

Consent Obligation *– Disclosure of personal data without consent*

20 April 2016

BACKGROUND

1 On 16 July 2014, the Personal Data Protection Commission ("Commission") received information that YESTUITION AGENCY (UEN 53084839B) ("Respondent") had disclosed on its website the NRIC numbers and images of certain individuals who had registered to be tutors with the Respondent and it was alleged that they had done so without the consent of the individuals concerned.

2 In light of the information received, the Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether there had been a breach by the Respondent of its obligations under the PDPA. The Commission's findings are set out below.

MATERIAL FACTS AND DOCUMENTS

3 The Respondent is a locally registered business providing home tuition matching services to individuals seeking tutors for primary to A-levels education. The Respondent renders its matching services via a website, which it operates at <www.yestuition.sg> ("Site").

4 The Site consists of various web pages that are accessible to the public and a tutors' login portal which is accessible only by individuals who had registered with the Respondent to be a tutor.

1 Act 26 of 2012.

Disclosure of NRIC numbers and images by the Respondent

5 From the Commission's examination of the Site, it was found that the Respondent had published images of its tutors on its Site. The tutors' images were stored in a JPEG file format and named using the tutors' respective NRIC particulars, for example, as 1234567A.jpg. As such, the Respondent had also disclosed the tutors' respective NRIC numbers with the images.

6 The NRIC numbers and images were at the material time made publicly discoverable and accessible via a directory listing on one of the Site's pages. Investigations by the Commission indicate that there were approximately 30 individuals whose images and NRIC numbers were listed by the Respondent in the directory listing.

The Respondent's responses to the Commission

7 In its responses to the Commission during the investigation, the Respondent represented that it had more than 10,000 tutors' profiles on its Site. It asserted that these profiles were not disclosed to members of the public.

8 The Respondent explained that individuals who wished to register with the Respondent as tutors were required to provide the following set of information to it by filling out a form made available on the Site ("Form"):

(a) full names;
(b) NRIC numbers;
(c) residential addresses;
(d) mobile numbers;
(e) e-mail addresses;
(f) education backgrounds; and
(g) relevant tutoring experiences.

9 Using the above information, the Respondent would then match the tutors to the appropriate students, and in return, collect a fee for the matching service.

10 The Respondent also represented to the Commission that tutors who submitted their personal data via the Site would have provided either their express or deemed consent to the collection, use and disclosure of their personal data by the Respondent for the purposes of providing the tutors

with tuition matching services. In this regard, the Commission notes that the Form expressly notified tutors that:

> By submitting this form, you hereby accept all terms & conditions as well as consent to be included in the mailing list of Yes Tuition to receive all information from us (Yes Tuition) electronically.
>
> Please be assured that we do not sell your personal information to third parties, and we will abide by our Privacy Policy.

11 The Commission also sets out below the more pertinent terms of the Respondent's privacy policy ("Privacy Policy"), which was referred to in the Form and available on the Respondent's Site at the material time, as follows:

> **Tutor**
> A tutor is a person who registers and maintains an account with Yes Tuition. *When you register as a tutor we ask for information such as your name, identification number, email address, passwords, telephone number, gender, occupation, qualification, and subjects you are interested to teach.* Once you register with Yes Tuition and sign in to our services, you are not anonymous to us. Tutors can go on-line to access their personal profile, and make changes to the subjects they are interested to teach and their personal information.
> …
>
> **Tutor**
> *Yes Tuition will not share personal information with any other third parties without your permission, unless required by, or in connection with, law enforcement action, subpoena or other litigation, or applicable law.* Yes Tuition will not sell, trade or lease your personal information to others.
>
> **Choice and Consent**
> *Yes Tuition does not require that you provide Yes Tuition with personal information. The decision to provide personal information is voluntary.* If you do not wish to provide the personal information requested, however, you may not be able to proceed with the activity or receive the benefit for which the personal information is being requested. Except as expressly stated otherwise in this Privacy Statement, *you may opt out of having Yes Tuition share personal information with third parties as described in this Privacy Statement by notifying Yes Tuition in writing of your desire to do so.*
> [emphasis added]

COMMISSION'S FINDINGS AND ASSESSMENT

Relevant issue

12 Under s 13 of the PDPA, organisations are prohibited from collecting, using or disclosing personal data about an individual unless:

(a) the individual gives, or is deemed to have given, consent under the PDPA to such collection, use or disclosure; or

(b) collection, use or disclosure of the personal data (as the case may be) is authorised or required under any written law.

13 In this case, the primary issue is whether the Respondent had the tutors' consent for the disclosure of their NRIC numbers and images to members of the public.

Commission's findings

14 As noted above, the Respondent collected several categories of personal data from its tutors. With the exception of the tutors' NRIC numbers and images, it generally did not disclose these data to members of the public. The Commission notes that this is in line with the terms of the Respondent's own Privacy Policy.

15 However, the Commission is of the view that the Respondent had not obtained its tutors' consent for disclosure of their images and NRIC numbers, which had been published on one of the pages of the Site. In this regard, the Commission further notes that such disclosure ran counter to the terms of the Respondent's own Privacy Policy.

16 In light of the foregoing, the Commission is of the view that the Respondent had disclosed the personal data of some of its tutors without their consent, and it is therefore in breach of s 13 of the PDPA.

ENFORCEMENT ACTION BY THE COMMISSION

17 Given the Commission's findings that the Respondent is in breach of its obligations under s 13 of the PDPA, the Commission is empowered under s 29 of the PDPA to give the Respondent 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 $1m as the Commission thinks fit.

18 In considering whether a direction should be given to the Respondent in this case, the Commission notes the following:

(a) the Respondent took proactive steps to restrict access to the relevant page containing personal data on the Site once it was made aware of the issue, and changed its practice of using its tutors' NRIC numbers as the file names of their images; and

(b) the Respondent had been co-operative with the Commission and forthcoming in its responses to the Commission during the Commission's investigation.

19 In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning against the Respondent for the breach of its obligations under s 13 of the PDPA.

20 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re Challenger Technologies Limited and another

Case Number: DP-1409-A103
Decision Citation: [2016] SGPDPC 6

Data intermediary *– Obligations of organisation and data intermediary*
Data intermediary *– "Processing" of personal data*
Protection Obligation *– Disclosure of personal data – Insufficient technical security arrangements*

20 April 2016

BACKGROUND

1 The Personal Data Protection Commission ("Commission") received a complaint from a member of the public on 15 September 2014 concerning an alleged data breach by Challenger Technologies Limited ("Challenger"). In brief, the Complainant alleged that Challenger had sent e-mail communications to members of its ValueClub programme, which contained the personal data of another ValueClub member.

2 The Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether there had been a breach by Challenger of its obligations under the PDPA.

3 In the course of its investigation, the Commission found that the e-mail communications in question (which were sent to Challenger's ValueClub members) had been sent by Xirlynx Innovations ("Xirlynx"), a business engaged by Challenger to handle all its e-mail communications to members of Challenger's ValueClub programme. The Commission's investigation therefore also examined whether there had been a breach by Xirlynx of its obligations under the PDPA.

4 The Commission's findings are set out below.

---

1 Act 26 of 2012.

MATERIAL FACTS AND DOCUMENTS

5 Challenger is a retailer of information technology ("IT") and other electronic products with several outlets around Singapore. As part of its customer relations efforts, Challenger established a customer membership programme known as ValueClub, which provides members with membership savings and discounts (amongst other benefits), and enables them to earn and accumulate ValueClub programme points which may be redeemed to offset the cost of purchases made at Challenger outlets.

6 Xirlynx is a third party IT vendor, which is registered and managed by its sole proprietor, [redacted] ("Mr T").

7 Some time in or around March 2010, Challenger engaged Xirlynx to manage and execute Challenger's e-mail campaigns under a contract for an "Email Blasting Package". The services provided by Xirlynx to Challenger under the contract included managing Challenger's ValueClub membership database and sending Challenger's weekly advertisements of promotions and monthly ValueClub e-statements to ValueClub members.

8 Challenger thereafter periodically renewed its "Email Blasting Package" contractual engagement with Xirlynx for the latter to send e-mail communications to ValueClub members, including the e-mail communications which are the subject of the Commission's present investigation.

9 In September 2014, Xirlynx sent the monthly ValueClub e-statements for that month to the ValueClub members by e-mail ("September E-mails"). However, many of the September E-mails contained personal data of another ValueClub member, including their name, expiry date of their ValueClub membership and total number of ValueClub programme points accumulated by the other member.

How the data breach occurred

10 In Challenger's responses to the Commission during the investigation, Challenger indicated that it had, upon being notified of the matter by the Commission, informed Mr T of Xirlynx about the alleged breach because Xirlynx managed Challenger's ValueClub membership database and was the party responsible for sending out e-mail communications to the ValueClub members. Challenger also conducted an internal investigation to ascertain the cause of the data breach.

11 Following its internal investigation, Challenger represented to the Commission that the root cause of the data breach was a processing error by their vendor, Xirlynx.

12 Challenger also represented to the Commission that it had taken remedial actions to inform the affected ValueClub members regarding the data breach and to rectify the mistakes caused by Xirlynx's error. In addition, Challenger represented that it had taken the extra precautionary step of terminating Xirlynx's services upon discovering the cause of the data breach, and it reviewed its ValueClub communication processes to prevent a reoccurrence of the data breach.

13 Separately, in Xirlynx's responses to the Commission during the investigation, Xirlynx explained that in September 2014, it had been instructed by Challenger to e-mail that month's ValueClub e-statements to ValueClub members. Xirlynx further explained that the following steps comprise its usual workflow for sending the ValueClub e-statements to ValueClub members:

(a) Xirlynx would receive a copy of the contents for the ValueClub e-statements from Challenger one day before the intended e-mail blast.

(b) Xirlynx would adapt the contents received from Challenger into a ValueClub e-statement HTML template. At this point, variables such as members' names, the expiry date of their ValueClub membership and their total number of existing ValueClub programme points, would have not yet been inserted into the HTML template.

(c) Xirlynx would then send the adapted layout to Challenger for its approval. Upon approval, Challenger would send to Xirlynx its updated ValueClub membership database with the latest ValueClub programme points for each member, listed in a text file (.txt) format.

(d) As Challenger's membership database contains duplicate e-mail addresses, Xirlynx would import the database into an Excel worksheet and remove any duplicates using Excel's "Remove Duplicates" function.

(e) The scrubbed database would then be imported into Xirlynx's e-mail blast system, and the ValueClub e-statements sent out to the ValueClub members.

14 For the September 2014 ValueClub e-statements, Xirlynx explained that it had carried out the usual steps listed above. However, while using the "Remove Duplicates" function in Excel to remove the e-mail duplicates from Challenger's membership database, Xirlynx admitted that it had inadvertently also caused an Excel column in the worksheet containing a list of ValueClub members' names, and an Excel column containing a list of the members' e-mail addresses, to be mismatched. This mix up resulted in some ValueClub members' personal data, specifically, their names, ValueClub membership expiry dates and ValueClub programme points, being sent to other ValueClub members in the September E-mails. In short, Xirlynx's error in the processing of the membership database led to the occurrence of the data breach.

15 Xirlynx informed the Commission that ValueClub e-statements with personal data of another ValueClub member had been sent to 165,306 ValueClub members. Xirlynx further represented that "only 34,230 recipients [of the September E-mails] that had opened the e-statements were affected". The Commission understands that Xirlynx derived this smaller number from its data on the number of ValueClub e-statements in the September E-mails which were actually accessed by the ValueClub members. The Commission notes that this does not take into account the possibility of additional members accessing the e-mails in the future. On balance, the Commission is of the view that since the September E-mails had been sent to 165,306 ValueClub members and would likely remain in their e-mail account until accessed or deleted by those members, it cannot be said that only 34,320 members were affected. The Commission therefore takes the view that 165,306 members' personal data had been disclosed to other members.

COMMISSION'S FINDINGS AND ASSESSMENT

Issues to be determined

16 The ValueClub e-statements sent in the September E-mails each contained a data set that identified another ValueClub member (who was an individual) by his or her full name, and provided the details of the member's accumulated ValueClub programme points and the expiry date of the member's ValueClub membership. The contents of the e-statements

therefore come within the definition of "personal data" in s 2(1) of the PDPA.[2]

17 Under s 24 of the PDPA, an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

18 Accordingly, a key issue in this case is whether Xirlynx had breached its obligations under s 24 of the PDPA.

19 Although Xirlynx had sent the September E-mails to ValueClub members, the Commission notes that Xirlynx was processing Challenger's ValueClub members' database and sending the September E-mails to the ValueClub members for Challenger pursuant to their contract. Related to this, s 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of personal data that is processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

20 As such, two additional issues in this case are:

(a) whether Xirlynx was a data intermediary of Challenger in respect of the events that caused the data breach; and

(b) if so, whether Challenger had breached its obligations under s 24 of the PDPA.

Commission's decision on the issues

Whether Xirlynx is a data intermediary of Challenger

21 Under s 2(1) of the PDPA, a "data intermediary" is an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.[3]

22 Section 2(1) also defines the term "processing", in relation to personal data, to mean the carrying out of any operation or set of operations in

2 See s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

3 See s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

relation to the personal data including, but not limited to, any of the following:

(a) recording;
(b) holding;
(c) organisation, adaptation or alteration;
(d) retrieval;
(e) combination;
(f) transmission;
(g) erasure or destruction.[4]

23 Having reviewed the "invoice no 2013-01549 from Xirlynx to Challenger dated 31 December 2013", and a "non-disclosure agreement dated 24 April 2014, entered into by [redacted] and [Mr T]) on behalf of Challenger and Xirlynx respectively" which was provided by Xirlynx to the Commission, and based on the facts set out at para 13, the Commission is of the view that Xirlynx had processed personal data of Challenger's ValueClub members pursuant to the arrangement between Xirlynx and Challenger and they had done so on behalf of Challenger. Further, Challenger had clearly relied on Xirlynx to process its ValueClub members' personal data to send the e-mail communications in question. Xirlynx was therefore a data intermediary of Challenger for the purposes of the PDPA.

24 As Xirlynx was a data intermediary of Challenger, Challenger has the same obligations under the PDPA in respect of Xirlynx's processing of personal data, as if the personal data had been processed by Challenger (*per* s 4(3) of the PDPA).

25 However, this does not affect Xirlynx's obligations under s 24 of the PDPA as that section applies equally to data intermediaries who process personal data on behalf of and for the purposes of another organisation pursuant to a contract in writing. In this regard, s 4(2) of the PDPA excludes the application of Pts III to VI of the PDPA, except for ss 24 and 25, to such data intermediaries.

4 See s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

Whether Xirlynx had breached section 24 of the PDPA

26 The fact that a data breach had occurred was undisputed by both Xirlynx and Challenger. The Commission therefore considered whether Xirlynx had made reasonable security arrangements to prevent the data breach from taking place.

27 From Xirlynx's representations to the Commission, it was clear that it fell on Xirlynx, as part of its e-mail blasting services, to ensure that the correct individualised ValueClub e-statement was sent to the correct intended recipient. Xirlynx's use of the Excel duplicate removal function while processing Challenger's ValueClub members database was part of this service.

28 It was therefore Xirlynx's responsibility to ensure that processing of Challenger's ValueClub members database was done in the correct manner so as to ensure that the correct set of personal data was sent by Xirlynx to each ValueClub member. The occurrence of the data breach is a *prima facie* indication that Xirlynx had not fulfilled its responsibilities in respect of processing and sending personal data.

29 The Commission further notes that Xirlynx's error could have been caught if it had proofread random samples of the ValueClub e-statements before the e-statements were sent out to verify that the names of the individuals in the e-statements matched the e-mail addresses to which the e-statements were sent.

30 Sample proofreading was a reasonable security arrangement that could have been conducted by Xirlynx given the nature of the services it provided, and which would likely have either averted the data leak or greatly reduced the number of individuals affected. The sample size should be appropriate relative to the total number of recipients.

31 Accordingly, the Commission takes the view that by failing to ensure that the correct personal data were sent to ValueClub members via the September E-mails, Xirlynx had breached its obligations under s 24 of the PDPA.

Whether Challenger had breached its obligation under section 24 of the PDPA

32 In light of the Commission's above finding that Xirlynx is a data intermediary of Challenger, it follows from s 4(3) of the PDPA that Challenger is obliged to protect the personal data administered by Xirlynx as if Challenger had processed the personal data itself. Section 4(3) of the PDPA states:

> An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary *as if the personal data were processed by the organisation itself*. [emphasis added]

33 The Commission's findings regarding the failure by Xirlynx to fulfil its responsibilities and obligations under the PDPA are therefore equally relevant in determining whether there was a breach of s 24 of the PDPA by Challenger.

34 In addition, the Commission notes that Challenger had heretofore neglected to exercise control over Xirlynx's workflow in the processing of Challenger's ValueClub membership database and the sending of e-mail communications to ValueClub members. Challenger had left it to Xirlynx to implement measures required to protect the personal data Xirlynx processed and, until the data breach occurred, had not considered what requirements it would want to implement to ensure that the personal data were appropriately protected, in accordance with s 24 of the PDPA.

35 Accordingly, the Commission is of the view that Challenger had similarly breached its obligation under s 24 of the PDPA.

ENFORCEMENT ACTION BY THE COMMISSION

36 Given the Commission's findings that both Challenger and Xirlynx were in breach of their respective obligations under s 24 of the PDPA, the Commission is empowered under s 29 of the PDPA to issue such directions as it deems fit to ensure compliance with the PDPA. This may include directing either or both parties to pay a financial penalty of such amount not exceeding $1m as the Commission thinks fit.

37 In considering whether to give such a direction in this case, the Commission notes the following:

(a) the personal data leaked were limited (comprising only ValueClub members' names, their membership expiry dates, and accumulated ValueClub programme points) and not of a sensitive nature;

(b) the personal data leaked could not be used by the individuals who had received them to profiteer or benefit from them, and was unlikely to lead to any harm or loss to the individuals concerned; and

(c) both Xirlynx and Challenger had been co-operative with the Commission and forthcoming in their responses to the Commission during the Commission's investigation.

38 The Commission also notes that Challenger had taken several proactive steps to remedy the breach, including engaging a new IT vendor and hiring the services of a data protection consultant.

39 In view of the factors noted above, the Commission has decided not to issue any direction to either Challenger or Xirlynx to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning to Challenger and Xirlynx respectively for the breach of their respective obligations under s 24 of the PDPA.

40 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re Metro Pte Ltd

Case Number: DP-1504-A421
Decision Citation: [2016] SGPDPC 7

Protection Obligation *– Access to personal data – Insufficient technical security arrangements*

20 April 2016

BACKGROUND

1 On 21 April 2015, the Complainant complained to the Personal Data Protection Commission ("Commission") that she had been receiving calls from unknown numbers, and that when she conducted a search on Google, she discovered that her personal data and those of her family members were posted online on <http://siph0n.net> ("Siph0n website"). The Complainant had attributed the posting on the Siph0n website to a data "leak" on the Respondent's part.

MATERIAL FACTS AND DOCUMENTS

2 On account of the complaint made, the Commission undertook an investigation, and sought the Respondent's response on the matter. The material facts of the case are as follows.

3 The Respondent had acknowledged that the personal data that were posted on the Siph0n website came from the database stored on its website, such data comprising personal data of individuals.[1]

---

1 "Personal data" under s 2 of the Personal Data Protection Act 2012 (Act 26 of 2012) means data, whether true or not, about an individual who can be identifed from that data; or from that data and other information to which the organisation has or is likely to have access.

4 The Respondent's corporate website was developed and supported by Grey Digital Southeast Asia (also known as Yolk Pte Ltd) ("Grey Digital"). The website was hosted by Limebox Hosting Solutions.

5 The Respondent's corporate website (<http://www.metro.com.sg>) was hacked into on 9 and 10 February 2014. Investigations were subsequently carried out by the Respondent's information technology ("IT") support partners, namely Grey Digital and Vodien Internet Solutions Pte Ltd ("Vodien"), into the hacking incidents. However, the investigations were unable to determine the cause of the February 2014 hacking incidents or the person(s) that had carried out the hacking(s). The Respondent produced to the Commission a report from Grey Digital in respect of the two hacking incidents ("Grey Digital's report"). The Commission understands that the Respondent had taken steps to improve on its web security following the hacking incidents in February 2014.

6 In March 2015, it was discovered that the names, personal e-mail addresses, NRIC numbers, personal mobile phone numbers, dates of birth and Facebook user IDs of the Respondent's customers were disclosed on the Siph0n website. This included the personal data of the Complainant and her family, which forms the subject of the complaint in this matter. The Respondent informed the Commission that the personal data that were posted on the Siph0n website were of 445 of its customers or users of the Respondent's website.

7 Following the March 2015 postings on the Siph0n website, the Respondent instructed Grey Digital to remove any user information from the server of the hacked corporate website.

8 The Respondent also engaged KPMG Singapore to carry out an assessment and audit of the security of its internal as well as external, *ie*, Internet-facing systems. A copy of the report dated 19 May 2015 was produced to the Commission on 10 July 2015 ("KPMG report").

9 During its investigations, the Commission was informed by the Respondent that it had resolved several of the IT security issues raised in the KPMG report and that it had intended to address/taken steps to address the remaining issues and to further improve on its website and server security.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Relevant issue in this case

10 Arising from the posting of personal data on the Siph0n website found in March 2015 and the IT security issues raised in the KPMG Report, the main issue in this case is whether the Respondent had in place reasonable security arrangements to protect the personal data in its possession or control, as required under s 24 of the Personal Data Protection Act 2012[2] ("PDPA"), when it came into effect on 2 July 2014.

11 Section 24 of the PDPA states that an organisation is obliged to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Section 24 of the PDPA came into effect on 2 July 2014.

Assessment of whether Respondent had complied with section 24 of the PDPA

12 The Commission notes that the Respondent has attributed the postings that were discovered in March 2015 to the two hacking incidents in February 2014. The Respondent thus took the view that there was no further breach for the disclosures on the Siph0n website made in March 2015 following the two incidents. The Commission, however, notes that the Respondent was under an obligation to ensure that reasonable security arrangements were put in place to protect the personal data under s 24 of the PDPA, when it came into force on 2 July 2014.

13 Despite the Respondent and/or Grey Digital apparently taking steps to improve the security of the Respondent's website and system following the two hacking incidents in February 2014, it was noted that the Respondent's system still contained numerous security issues and vulnerabilities when the security scan was conducted from March 2015 to May 2015. This is evidenced by the KPMG report dated 19 May 2015 that was produced to the Commission by the Respondent.

---

2 Act 26 of 2012.

14 In the KPMG report, KPMG had found 30 issues with the system, comprising of six "Significant Issues", 11 "Reportable Issues" and 13 "Observations". Amongst the issues raised, the Commission notes that there were three significant issues and one reportable issue with the external web application security, and one reportable issue in relation to the external network security.

15 In this regard, there was at least one signfiicant issue in the KPMG report which is indicative of a failure of reasonable security arrangements even as of 19 May 2015. This is the SQL injection vulnerability. The Commission understands that the SQL injection vulnerability would have been found in the programming code of the Respondent's external web applications, and may have been present in these web applications from the outset. In the Commission's view, this is a common and well-documented form of vulnerability that ought to have been reasonably anticipated, identified and rectified by the Respondent at an early stage.

16 The Commission also notes that even as of 19 May 2015, the Respondent's web servers were accessible to the Internet; and hosted the Respondent's website, which is the interface from which the Respondent had collected and stored the personal data from its users or customers. Accordingly, any vulnerability in the web servers or the web applications would pose a real risk or threat to the security of the personal data that were collected and/or held by the organisation. It was therefore imperative that the Respondent take the necessary measures to ensure that the servers and web applications themselves would be secure and free from any known significant security risks or vulnerabilities. The fact that there were a number of issues with the security of the Respondent's IT system, particularly, the SQL injection vulnerability, indicated to the Commission that the web security was lacking. The Commission notes that the personal data from the previously affected database (*ie*, the database which was hacked) was only transferred from the Internet-facing webservers after the postings to the Siph0n website in March 2015.

17 Based on the above, the Commission finds that the Respondent had failed to make reasonable security arrangements to protect the personal data held in its web servers, and it is therefore in breach of s 24 of the PDPA.

ACTIONS TAKEN BY THE COMMISSION

18 Given the Commission's findings that the Respondent is in breach of its obligations under s 24 of the PDPA, the Commission is empowered under s 29 of the PDPA to give the Respondent 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 $1m as the Commission thinks fit.

19 In considering whether a direction should be made or given to the Respondent in this case, the Commission notes that:

(a) the Respondent had taken action to strengthen the security of its website, including engaging KPMG to undertake an internal IT security audit and assessment shortly after it had learnt of the posting of its customer's or user's personal data on the Siph0n website. However, the Respondent's actions (after the hacking incidents in February 2014) did not enable it to detect and address at least one significant security lapse until several months later (*ie*, after May 2015).

(b) the data leak that gave rise to the complaint took place before July 2014, and there is no evidence that there has been a data breach to date, notwithstanding the Respondent's failure to make reasonable security arrangements.

20 In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning against the Respondent for the breach of its obligations under s 24 of the PDPA.

21 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re Full House Communications Pte Ltd

Case Number: DP-1503-A368
Decision Citation: [2016] SGPDPC 8

Protection Obligation *– Access to personal data – Insufficient technical, physical and administrative security arrangements*

20 April 2016

INTRODUCTION

1 The Complainant submitted a complaint to the Personal Data Protection Commission ("Commission") on 4 March 2015 in respect of the way that the Respondent had collected and protected[1] personal data[2] at a lucky draw redemption counter operated by the Respondent. The specific matters that were raised in his complaint were as follows:

> (a) The auto-fill function was enabled for the forms on the Respondent's laptops that a participant had to fill up to register for the lucky draw. This allowed a user to view from a drop-down box the historical entries containing the personal information of the previous registering participants.
> (b) The Respondent's laptop screens were in plain view of customers waiting in line behind the Complainant, which allowed them to view the personal information that was being entered into the laptop.

---

1 Section 24 of the Personal Data Protection Act 2012 (Act 26 of 2012) states that an organisation is obliged to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Section 24 came into effect on 2 July 2014.

2 "Personal data" as referred to in s 24 of the Personal Data Protection Act 2012 (Act 26 of 2012) refers to data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.

(c) The page containing the form was accessed through an unsecured Mozilla Firefox browser at the site: <http://localhost/coupon/finish.php>.

(d) The Respondent's staff did not appear to be adequately trained to ensure the protection of personal data collected at the redemption counter.

MATERIAL FACTS AND DOCUMENTS

2 The lucky draw that the Respondent had organised was for a furniture fair that took place from 28 February 2015 to 8 March 2015 at the Singapore Expo Hall 7 ("Furniture Fair"). On 1 March 2015, the Complainant and his mother had attended the Furniture Fair and had purchased items which entitled the Complainant to participate in the Respondent's lucky draw. To participate in the lucky draw, a participant was required to register his personal details on the laptops provided by the Respondent at the redemption counter, including the individual's name, identity card number, occupation, contact number, e-mail address and residential address. The form would then be printed out and dropped into a box for the lucky draw.

3 While entering the personal details of his mother in the computerised form, the Complainant had four main concerns about the level of protection of the personal data that was provided by the Respondent, as mentioned at [1] above.

4 Following from the Commission's investigation into the matter, the Respondent's responses to the Commission were, in essence, as follow:

(a) The Respondent acknowledged that the auto-fill function had been enabled for all the fields in the form for the convenience of customers.

(b) The Respondent maintained that the personal data entry into the laptops had been in the presence of its staff, and they would watch the customers and ensure that no one would be able to take photos of the personal information displayed on the laptops.

(c) The forms were not accessible to the Internet.

(d) Subsequent to receiving the Commission's notification of this matter, the Respondent had taken remedial actions during the ongoing Furniture Fair.

5 The Commission also understands that the Respondent had taken remedial actions as follow:

(a) The Respondent said it changed its practices by having the entries into the forms on the laptops made by its staff instead of by the registering participants themselves.

(b) The Respondent also said that it had reconfigured the table arrangements so that the screens of the laptops were aligned away from the view of registering participants in queue at the redemption counter.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

6 The Commission's findings on the four issues raised are as follows.

Issues at [1(a)] and [1(d)]: The Respondent's failure to protect personal data by enabling the auto-fill function and the failure of the Respondent's staff to protect personal data

7 In the Commission's assessment, by enabling the auto-fill function, this permitted a user to have access to the personal data of other individual(s) that were stored on the Respondent's laptops.

8 The Respondent has pointed out that the information that a user would have access to was confined to information found within that particular drop-down box, and that the entries were not listed in chronological order of the time that they were entered into the system. In this regard, it would be difficult to draw a connection between the entries in the various drop-down boxes to link them to a particular individual. It follows from this line of argument that the information that a user would have access to would not be personal data, but simply generic information, and hence the Respondent was not in breach of s 24 of the Personal Data Protection Act 2012[3] ("PDPA").

9 The Commission disagrees with this line of argument. It was noted that the information that was displayed in the drop-down boxes included the individual's name, identity card number, contact number and e-mail address. Based on the definition of "personal data" under the PDPA, some

3 Act 26 of 2012.

of this information would, by itself or collectively, amount to personal data. For example, by having a person's full name in the drop-down box alone, one would be able to identify the person who had registered as a participant of the Furniture Fair. Therefore, even if a person had access to the information in a single drop-down box, that may be sufficient in identifying an individual.

10 The Commission also notes that there may be certain instances where a link could be drawn between the information across fields – *ie*, such as the instance where an e-mail address containing part of the individual's name could be linked to the full name of the individual, and hence, identify that individual.

11 In the premises, the Commission finds that by enabling the auto-fill function for the drop-down boxes, the Respondent had failed to make reasonable security arrangements under s 24 of the PDPA.

12 While the Respondent claimed that its staff had been present to monitor unauthorised user access to data stored in the system, however, the Commission notes that the Respondent was providing the very function itself (by enabling the auto-fill function) that would allow a user access to personal data of the other individuals. In this regard, the Commission is of the view that the staff presence (if any) would not have made any difference in preventing any user from accessing the personal data stored on the system.

13 Notwithstanding the Commission's view about the presence of the staff at the redemption counter, the Commission makes no finding on the other allegation raised by the Complainant at [1(d)] above (*ie*, that the Respondent's staff could not ensure the protection of personal data), as there was no evidence of an actual failure by the Respondent's staff to protect the personal data collected by the laptops.

Issue at [1(b)]: Laptop screens were in plain view of other customers

14 In relation to the allegation that the Respondent's laptop screens were in plain view of the other customers, the Commission notes that there is no evidence that other customers could easily observe the information displayed on the laptop screens. The Commission further notes the assurance given by the Respondent that its staff was on hand to watch over the laptops and, in particular, to ensure that other individuals did not take

photographs of the laptop screens. The Commission therefore makes no finding in respect of this allegation.

Issue at [1(c)]: Computerised forms accessed through unsecured Mozilla Firefox browsers

15 In respect of the allegation that the computerised forms were accessed through unsecured Mozilla Firefox browsers, the Commission notes that the forms and the personal data were collected and stored on the local hard drives and were not accessible on the Internet. The Commission is of the view that the risk of online attacks or intrusion to these laptops where the personal data were held could not be ascertained. The Commission therefore makes no finding in respect of this allegation.

ACTIONS TAKEN BY THE COMMISSION

16 Given the Commission's findings that the Respondent is in breach of its obligations under s 24 of the PDPA, the Commission is empowered under s 29 of the PDPA to give the Respondent 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 $1m as the Commission thinks fit.

17 In considering whether a direction should be made or given to the Respondent in this case, the Commission notes that: (a) the impact of the breach is limited, since, in the given circumstances, a user would have had limited time to observe and collect personal data in the drop-down boxes; and (b) the Respondent took action shortly after the complaint was made to stop the use of the drop-down boxes and to arrange for its staff to fill in the forms themselves.

18 In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning against the Respondent for the breach of its obligations under s 24 of the PDPA.

19 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re Singapore Computer Society

Case Number: DP-1504-A390
Decision Citation: [2016] SGPDPC 9

Protection Obligation *– Disclosure of personal data – Insufficient technical and administrative security arrangements*

20 April 2016

BACKGROUND

1 On 17 March 2015, the Respondent notified the Personal Data Protection Commission ("Commission") that it inadvertently disclosed certain personal data of individuals attending an event organised by the Respondent to other individuals and had received information about the disclosure from some of the individuals concerned. After being notified of the incident by the Respondent, the Commission undertook an investigation to determine whether there had been a breach of the Personal Data Protection Act 2012[1] ("PDPA"). The material facts of the case are as follows.

MATERIAL FACTS AND DOCUMENTS

2 In April 2015, the Respondent jointly organised and conducted an event with the Infocomm Development of Singapore ("IDA") named "IDEAS on Security Analytics". Prior to the event, on 16 March 2015, an employee of the Respondent, [redacted] ("Ms L"), sent out an e-mail to all individuals who had registered to attend the event ("registrants"), which had attached a copy of the registration list for the event. The registration list contained personal data of about 214 registrants (individuals). Eleven of the registrants subsequently raised concerns about the unauthorised disclosure of their personal data to the Respondent. The personal data which had been

1 Act 26 of 2012.

disclosed included information such as the registrants' full names, NRIC numbers, contact numbers, e-mail addresses, organisation and designation information. The Respondent confirmed that it was not acting on behalf of IDA in relation to the collection, use, disclosure or processing of the registrants' personal data.

3 The Respondent acknowledged to the Commission that the registration list was not meant to be disclosed externally and had been inadvertently sent to registrants on 16 March 2015. The Respondent explained that Ms L's supervisor (who was also an employee of the Respondent) had sent her the registration list in an e-mail which included a draft event confirmation e-mail which Ms L was required to send to registrants. Ms L used the "Forward" function in her e-mail application to send the event confirmation e-mail on 16 March 2015 but forgot to remove the attached registration list (which was automatically attached to her e-mail to registrants by her use of the "Forward" function).

4 Upon being notified of the disclosure by some registrants, the Respondent took the immediate step of initiating an e-mail recall at 3.00pm on 16 March 2015, approximately 40 minutes after the e-mail with the registration list was sent.

5 The Respondent's data protection officer subsequently sent an official e-mail apology to the 11 registrants who had raised concerns to the Respondent over the incident. All 11 registrants accepted the apology and did not pursue the matter further. Neither the Respondent nor the Commission received other complaints relating to this incident.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Relevant issue(s) in this case

6 This case principally concerns an unauthorised disclosure of personal data by an employee of the Respondent. Under s 24 of the PDPA, an organisation is required to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised disclosure, disposal, access, collection, use or similar risks (amongst others).

7 A secondary issue in this case is that the Respondent did not have the consent of the registrants to disclose their personal data to other registrants (as required under s 13 of the PDPA). However, as the Respondent never intended to make such a disclosure, and hence would not have sought consent from the registrants, the Commission notes that this case is more properly considered from the perspective of the Respondent's obligations under s 24 of the PDPA. Nevertheless, the Commission is not precluding that other cases may require an examination of both ss 13 and 24.

Commission's findings on the relevant issue(s)

8 It is not disputed by the Respondent that its employee, Ms L, had made an unauthorised disclosure of registrants' personal data to other registrants via her e-mail of 16 March 2015. The Commission notes that this unauthorised disclosure arose from a number of factors which reflect poor data handling practices by the Respondent, including the following:

(a) Ms L's supervisor had sent her the registration list containing registrants' personal data in the same e-mail which contained a draft event confirmation e-mail which Ms L was required to send to registrants. This gave rise to a risk that Ms L may either not realise the registration list was attached or may forget to delete the registration list when she used the "Forward" function in the e-mail application to send the event confirmation e-mail; and

(b) the registration list sent to Ms L was not protected by a password (or in any other manner which would prevent unintended recipients from opening it and accessing the data contained therein).

9 Under s 53(1) of the PDPA, any act done, or conduct engaged in, by an employee shall be treated for the purposes of the PDPA as acts done, or conduct engaged in, by his employer as well as him. The Respondent is therefore liable for the acts and conduct of its employees in relation to the unauthorised disclosure of registrants' personal data on 16 March 2015.

10 In relation to the personal data which had been disclosed by the Respondent on 16 March 2015, the Commission notes that a significant amount may be business contact information, which is defined in s 2 of the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not

provided by the individual solely for his personal purposes". For personal data which are business contact information, s 4(5) of the PDPA provides that Pts III to VI of the PDPA, which include s 24, do not apply. Nevertheless, as at least some of the personal data disclosed, for example, the NRIC numbers of registrants, were not business contact information, the Respondent was required to protect such personal data in accordance with s 24.

11 Overall, the Commission considers that the Respondent's data handling practices in relation to the sending of the event confirmation e-mail to registrants did not include sufficient security arrangements to the standard required under s 24 of the PDPA. The Commission therefore finds that the Respondent is in breach of s 24 of the PDPA.

ACTIONS TAKEN BY THE COMMISSION

12 The Commission is empowered under s 29 of the PDPA to give the Respondent such directions as it deems fit to ensure the Respondent's compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding $1m as the Commission thinks fit.

13 In considering whether a direction should be given to the Respondent in this case, the Commission notes the following:

(a) a significant part of the personal data disclosed was business contact information;

(b) the Respondent took prompt action to recall the e-mails of 16 March 2015 which had the attached registration list, even though this process did not result in a complete recall of all the e-mails; and

(c) the Respondent informed the PDPC of the data breach voluntarily and was co-operative during the investigation.

14 In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent under s 29 of the PDPA. Instead, the Commission has decided to issue a Warning to the Respondent for the breach of its obligations under s 24 of the PDPA.

15 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re AIA Singapore Private Limited

Case Number: DP-1509-A533
Decision Citation: [2016] SGPDPC 10

Consent Obligation *– Disclosure of personal data without consent*
Continued use of personal data after appointed day
Notification Obligation *– Disclosure of personal data without notification*
Purpose Limitation Obligation *– Disclosure of personal data for purposes that a reasonable person would consider appropriate in the circumstances*

22 June 2016

BACKGROUND

1 On 18 September 2015, the Personal Data Protection Commission ("Commission") received a complaint from the Complainant, alleging that the Respondent had made an unauthorised disclosure of his personal data, in particular, his bank account details, to Chiropractic First CFG (TP) Pte Ltd ("CFG") in respect of the Complainant's claim under an insurance policy.

2 The Commission investigated into the alleged unauthorised disclosure made, and its findings are set out below.

MATERIAL FACTS AND DOCUMENTS

3 The Respondent is an insurance company. The Complainant holds an insurance policy with the Respondent. Previously, in signing up for the insurance policy with the Respondent, the Complainant provided information about himself in the application form ("Application Form"), including his name, address, NRIC number, contact details, occupation and various other personal particulars ("Personal Particulars").

4 In the declaration portion of the Application Form, the Complainant agreed, amongst other things, to the Respondent: (a) releasing to any medical source or insurance office any relevant information concerning the

Complainant at any time; and (b) using and/or disclosing any information to independent third parties with regard to any matters pertaining to the application/policy.

5 On 24 May 2015, the Complainant made a claim for insurance under the policy with the Respondent. In raising the claim, the Complainant had to fill in an accident and hospitalisation claim form ("A&H Form") to be submitted to the Respondent. In the A&H Form, the Complainant had to provide, amongst other things, his policy details, his Personal Particulars, and his bank account information "for direct crediting of claims". For the bank account information, the Complainant provided the name of the bank, branch of the bank, the bank account number and the account holder's name ("Bank Account Details").

6 In the authorisation and declaration portion of the A&H Form, the Complainant had agreed, amongst other things, to the Respondent disclosing the personal data of the Complainant for purposes described in the "AIA Personal Data Policy".

7 The AIA Personal Data Policy ("Policy") produced by the Respondent sets out the following scope of consent:

> (a) The persons who may be provided with the insured's personal data. Specifically, it states that the Respondent may disclose personal data to "medical sources and insurance organisations".
> (b) The types of personal data that may be collected, used or disclosed, including the insured's "personal particulars such as NRIC numbers, passport numbers, contact details, addresses, date of birth, occupation, photographs and marital status" or "your financial information such as income, bank account numbers, CPF statements, bank statements".
> (c) The purposes for which personal data may be collected, used or disclosed. In particular, it lists the purpose to "assess, process, administer, implement and effect the requests or transactions" or "assessing, processing, settling, authenticating and investigating claims".

8 Pursuant to the Complainant's claim, the Respondent had communicated with the Complainant's chiropractor, CFG, to obtain further medical information about the Complainant. In its communication, the Respondent disclosed pp 1 and 3 of the A&H Form to CFG, which disclosed, amongst other things, the Complainant's Bank Account Details.

9 According to the Respondent, there were a number of reasons why it was permitted or authorised to disclose the personal data of the Complainant to CFG. Briefly, the Respondent claimed that:

(a) The Complainant had provided consent for his personal data to be disclosed to CFG, pursuant to the A&H Form read with the Policy.

(b) The disclosure was necessary to; (i) facilitate the speedy processing of the claim; (ii) assure CFG that the Respondent's request for disclosure is based on a claim from CFG's patient/the Respondent's policy holder, and (iii) assure CFG that all required consents had been obtained to allow CFG to respond to the Respondent's requested information.

(c) CFG would be obliged to handle the information that the Respondent had provided in a manner that ensures its confidentiality.

(d) The disclosure was consistent with s 20(2) of the Personal Data Protection Act 2012[1] ("PDPA") which states that an organisation, on or before disclosing personal data about an individual from another organisation without the consent of the individual, shall provide that other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with the PDPA.

(e) The Complainant was, according to the Respondent, a former financial services consultant "appointed by" the Respondent. He is therefore aware of the claims processing procedure, and would be, at the very least, deemed to have consented to the Respondent's collection, use and disclosure of his personal data for claims processing by reason of his former appointment or engagement.

COMMISSION'S FINDINGS AND ASSESSMENT

10 The issues in this case to be determined are as follow:

(a) Pursuant to ss 13, 14, 15 and 20 of the PDPA, did the Respondent provide the necessary notification and obtain the necessary consent from the Complainant before disclosing pp 1 and 3

1 Act 26 of 2012.

of the A&H Form to CFG, in particular the Complainant's Bank Account Details?

(b) If not, is the Respondent able to rely on any of the exceptions under the PDPA for the disclosure?

(c) Further, can the disclosure of the Bank Account Details contained on p 1 of the A&H Form to CFG be said to be "for purposes that a reasonable person would consider appropriate in the circumstances" under s 18(*a*) of the PDPA?

Issue (a): Notifying the Complainant and obtaining consent for the disclosure of A&H Form

11 The authorisation and declaration sections of the Application Form, A&H Form and the Policy are broadly worded and a plain reading leads to the conclusion that the consent obtained by the Respondent under the Application Form, A&H Form and Policy is wide enough to cover the disclosure made by the Respondent of pp 1 and 3 of the A&H Form to CFG. On this assessment of the relevant clauses produced before the Commission, the Commission finds that the Respondent had the Complainant's *consent*, for the purposes of the PDPA, to disclose the majority of personal data contained in pp 1 and 3 of the A&H Form to CFG, save for the Bank Account Details.

12 With regards to the Bank Account Details, the section of the A&H Form in which the Bank Account Details were to be entered expressly states that the Bank Account Details were for "direct crediting of claims". This purpose is at odds with and constrains the otherwise broad consent clauses in the Application Form, A&H Form and the Policy. Specific to this case, it does not extend to permitting the Respondent to disclose the Bank Account Details for the purpose of obtaining a medical report from third parties. This casts doubts as to whether the Complainant had in fact given his consent for such disclosure. On balance, the Commission is unable to draw a firm conclusion on whether the phrase "direct crediting of claims" was intended to and did in fact constrain the broad consent previously obtained by the Respondent or that the Complainant had effectively given his consent for the disclosure of his Bank Account Details for the purpose of obtaining a medical report. In the final analysis, the Commission thought it was prudent to decline making a finding of breach on the issue in the absence of clear supporting evidence. Further, the Commission's findings in

respect of the issue of whether the disclosure of Bank Account Details accords with s 18 of the PDPA, as will be examined below, make it unnecessary to do so.

13 With regard to whether the Respondent had given sufficient *notification* to the Complainant for disclosing the Complainant's personal data for purposes of the Complainant's claim, the Commission is of the view that the A&H Form (and Policy) can possibly operate as prior notification for such a disclosure to be made.

14 In the premises, the Commission finds that the Respondent has complied with its obligations under ss 13, 14, 15 and 20 of the PDPA to provide the necessary notifications and obtain the necessary consent for the disclosure of the personal data (save for the Bank Account Details) found at pp 1 and 3 of the A&H Form to CFG. In relation to the Bank Account Details, on a balance, the Commission finds that there is insufficient evidence to show that the Respondent had failed to comply with its obligations under ss 13, 14, 15 and 20 of the PDPA.

Issue (b): Applicable exceptions and section 19 of the PDPA

15 For completeness, the Commission also considered the applicability of s 19 of the PDPA. Section 19 of the PDPA provides that an organisation may use personal data about an individual collected before the appointed day (*ie*, 2 July 2014) for the purposes for which the personal data were collected unless (a) consent for such use is withdrawn in accordance with s 16 of the PDPA; or (b) the individual, whether before, on or after the appointed day, has otherwise indicated to the organisation that he does not consent to the use of the personal data.

16 In this case, the Complainant had provided his Personal Particulars in the Application Form to sign up for the insurance policy with the Respondent in 2011, and agreed to the terms set out in the Application Form, which provided for the Respondent to use the Complainant's personal data for a variety of purposes mentioned at [4] above. Since the Personal Particulars were provided before the appointed day, pursuant to s 19 of the PDPA, the Respondent was allowed to continue using them based on the terms of the Application Form, which includes disclosing the data to CFG for the purposes of obtaining a medical report for the insurance claim.

17 However, s 19 of the PDPA does not apply to the Bank Account Details as they were not collected through the Application Form but through the A&H Form on 24 May 2015.

Issue (c): Disclosure of personal data was not for purposes reasonable or appropriate in the circumstances

18 Section 18 of the PDPA provides, *inter alia*, that 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. It should be borne in mind that s 18 of the PDPA is an independent obligation that the organisation would need to comply with even if it had obtained the consent from the relevant individual for the collection, use or disclosure of his personal data. This is an important aspect of the PDPA as it is effective in addressing excesses in the collection, use or disclosure of personal data under a broadly-worded consent clause, like in the present case.

19 In this case, the Bank Account Details of the Complainant were found at p 1 of the A&H Form that was disclosed to CFG. In the Commission's view, the disclosure of the Bank Account Details by the Respondent was not for "a purpose that a reasonable person would consider appropriate in the circumstances" under s 18 of the PDPA. The disclosure of the Bank Account Details was not relevant or necessary to the request for a medical report from CFG. Of the reasons provided by the Respondent (and set out at [9] above), the most pertinent one is that of facilitating speedy processing of the claim. It is not obvious how the Bank Account Details are relevant to CFG's role in the claim process, nor is it obvious how the Bank Account Details will assist CFG in turning out its medical report sooner. In any event, the Bank Account Details are necessary for the purpose of effecting payment, which is a function that is logically not within CFG's domain but which falls on the Respondent. Ultimately, the Respondent has not provided any reasonable explanation for why the disclosure of the Bank Account Details needed to be made in the circumstances. In the Commission's view, it was unsatisfactory for the Respondent to disclose sensitive personal data of a financial nature to a third party without good reason or purpose.

20 As discussed above, although the authorisation and declaration portion of the A&H Form provides for a broad-range of actions that may

be taken in respect of the personal data provided, the section of the A&H Form in which the Bank Account Details were to be entered states that the Bank Account Details were for "direct crediting of claims". The disclosure made therefore was for a purpose wholly different from this section of the form. Neither can it be said that the purpose of obtaining a medical report is one that is reasonably connected to this antecedent purpose. In the overall circumstances, it was not appropriate for the Respondent to be disclosing the Bank Account Details for a purpose that has no reasonable connection to that which was stated on the A&H Form.

21 In the premises, the Commission finds that the Respondent was in breach of s 18 of the PDPA for the disclosure of the Complainant's Bank Account Details to CFG.

22 In respect of the other personal data that was provided in pps 1 and 3 of the A&H Form, the Commission is of the view that the disclosure was made reasonably under s 18 of the PDPA as the Personal Particulars have clear relevance to and will facilitate the process of preparing a medical report.

ENFORCEMENT ACTION TAKEN BY THE COMMISSION

23 Given the Commission's findings that the Respondent is in breach of its obligations under s 18 of the PDPA, the Commission is empowered under s 29 of the PDPA to give the Respondent 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 $1m as the Commission thinks fit.

24 On a balance, the Commission has decided not to impose a financial penalty on the Respondent in view of the overall circumstances of the matter. Instead, the Commission has decided to issue a Warning to the Respondent. In coming to this decision, the Commission has taken into account the following considerations:

(a) the disclosure was limited to a single third party, CFG, and the personal data, as to which the unauthorised disclosure was made, although of a sensitive financial nature, were limited to a single data set, *ie*, the Bank Account Details;

(b) the disclosure had been under circumstances in which CFG knew that the personal data disclosed were to be treated confidentially;

(c) there was no evidence of actual loss or damage suffered by the Complainant from the disclosure made; and

(d) the Respondent had undertaken an immediate review of its processes in relation to the disclosure of personal data to parties following the incident.

25 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.

LEONG KENG THAI
Chairman
Personal Data Protection Commission

Grounds of Decision

Re Central Depository (Pte) Limited and another

Case Number: DP-1506-A456
Decision Citation: [2016] SGPDPC 11

Data intermediary *– Obligations of organisation and data intermediary*
Protection Obligation *– Disclosure of personal data*

21 July 2016

BACKGROUND

1 On 11 June 2015, the Central Depository Pte Limited ("CDP") reported to the Personal Data Protection Commission ("Commission") an incident of a data breach involving its customers' personal data. It was reported that six CDP account holders had received CDP account statements for the month of May 2015 containing account information of other account holders. On the same day, Singapore Exchange Limited ("SGX") issued a news release to inform and apologise for the incident.

2 Following the reporting of the incident, the Commission undertook an investigation into the matter. The Commission had determined that the two Respondents in the matter were CDP and Toh-Shi Printing Singapore Pte Ltd ("Toh-Shi") respectively. The Commission's decision on the matter and grounds of decision are set out below.

MATERIAL FACTS AND DOCUMENTS

3 CDP is a wholly-owned subsidiary of SGX, and provides clearing, settlement and depository facilities in the Singapore securities market. Toh-Shi is the external vendor of CDP in charge of printing the CDP account statements for CDP.

4 The printing services provided by Toh-Shi are governed by a contract between the parties dated 1 March 2013 (the Document Management Service Agreement ("DMSA")). The DMSA required, amongst other things, for Toh-Shi to protect the confidentiality of the CDP account

holders' personal data and to put in place the necessary measures to protect the data.

5 Following the discovery of the data breach and Toh-Shi alerting the Commission of the breach, on 15 June 2015, CDP reissued the corrected CDP statements for the month of May 2015 with an apology letter to the 195 affected account holders. On 17 June 2015, SGX started to contact the affected account holders to assist with any queries or concerns, and to give them an option to change their CDP account numbers. From what the Commission understands, none of the account holders requested to change their account numbers.

6 On 26 June 2015, SGX conducted its own internal investigation into the incident and provided the SGX Regulatory Breach Report to the Commission.

7 Based on the investigations that were carried out, SGX found that the data breach incident occurred due to a misalignment of the pages during the sorting process which led to errors in the compilation of multi-page CDP statements such that the first page of the statement of one account holder was compiled with the second and subsequent pages of another account holder. The erroneous pages were initially spotted and marked out by Toh-Shi's print system operator ("PSO"). He subsequently informed the fan fold operator ("FFO") of the markings; who was to discard the erroneous statements and to replace them with the correct statements from the printed roll. However, the FFO had mistakenly discarded the correct statements and despatched the erroneous statements for postage instead. This led to the erroneous statements being mailed to the account holders.

8 According to SGX's own internal investigation, 92 out of the 195 affected CDP account holders had received the second page belonging to another account holder containing one or more of the following information:

(a) account information (*ie*, name, address and account number);
(b) securities holdings;
(c) transaction summary; and/or
(d) payment summary.

9 The remaining 103 affected CDP account holders received the second page containing account information of another account holder and general

CDP information, with no details on securities holdings, transactions or payments.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

10 The issues in this case to be determined are as follow:

(a) What obligations did CDP and Toh-Shi each owe under the Personal Data Protection Act 2012[1] ("PDPA") in respect of the personal data of the CDP account holders?

(b) Did CDP comply with its obligation under s 24 of the PDPA in respect of the data breach incident that happened?

(c) Did Toh-Shi comply with its obligation under s 24 of the PDPA in respect of the data breach incident that happened?

Relevant provisions under the PDPA

11 Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

12 Section 4(2) of the PDPA provides that Pts III to VI (except for s 24 of the PDPA (protection of personal data) and s 25 of the PDPA (retention of personal data)) shall not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

13 Section 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

1 Act 26 of 2012.

The relationship between CDP and Toh-Shi and their respective obligations under the PDPA

14 The Commission notes that Toh-Shi is responsible for printing the account statements of CDP's account holders (containing their personal data) for CDP. This involves CDP providing to Toh-Shi personal particulars and stock holdings of account holders and statement document templates. Toh-Shi has to manage the entire process of merging account statement data with the correct statement document template and printing the final account statement. In this regard, Toh-Shi was carrying out activities of "processing" the personal data on behalf of CDP, as defined by the PDPA. Accordingly, the Commission finds that Toh-Shi was acting as a data intermediary for CDP.

15 Pursuant to ss 4(2) and 4(3) of the PDPA, both CDP and Toh-Shi are obliged under s 24 of the PDPA to ensure that there are reasonable security arrangements to protect the personal data of CDP's account holders.

16 The Commission now turns to its assessment of whether CDP and Toh-Shi have complied with their obligations under s 24 of the PDPA respectively.

Whether CDP has complied with its obligations under section 24 of the PDPA

17 Based on the Commission's investigation into the matter, it is satisfied that CDP had complied with its obligations under s 24 of the PDPA. In particular, the Commission notes that CDP had in place an agreement obliging Toh-Shi to take the necessary actions and precautionary measures to protect the CDP account holders' personal data during the printing process. On CDP's part, it was noted that CDP had in place processes for the secure transfer of personal data between CDP and Toh-Shi: CDP ensured that the files containing the CDP account holders' personal data were sent to Toh-Shi via a secured format, *ie*, Secured File Transfer Protocol.

18 Accordingly, the Commission does not find CDP in breach of s 24 of the PDPA.

Whether Toh-Shi has complied with its obligations under section 24 of the PDPA

19 The Commission notes that the cause of the breach in this case was due to error(s) made by the staff of Toh-Shi during the printing process.

20 In the Commission's assessment, the breach occurred as a result of inadequate operational processes in place to ensure that the letters and personal data were sent to the correct recipient. The Commission notes that in this case the PSO had manually checked that the correct CDP statements were printed and in the event that there was any error, the PSO would mark out the erroneous ones and provide the FFO with both the erroneous and correct CDP statements for sorting. As only one person was involved in the sorting, it resulted in the FFO discarding the correct CDP statements instead of the erroneous ones. In the Commission's view, the measures to sort manually by one person were insufficient given the nature of the personal data involved. The human error in this case could have been avoided by putting in place processes or technology solutions that can minimise human error.

21 The Commission notes that following the data breach incident, Toh-Shi had taken steps to improve on the security of the system by implementing (a) additional layers of checks by a supervisor, quality controller and the manager; (b) a barcode system; and (c) a technology solution to automate the reconciliation of the printed statements to prevent a repeat of the incident. In the Commission's view, if there were a better system of checks in place, the data breach incident could have been prevented.

ENFORCEMENT ACTION TAKEN AGAINST TOH-SHI

22 Given the above, the Commission finds that CDP is not in breach of s 24 of the PDPA. However, the Commission finds that Toh-Shi is in breach of s 24 of the PDPA.

23 In exercise of the power conferred upon the Commission pursuant to s 29 of the PDPA, the Commission directs that a financial penalty of $5,000 be meted out against Toh-Shi.

24 In coming to the direction to be given, the Commission has taken into consideration the overall circumstances of the matter, namely:

(a) A considerable number of individuals (totalling 195) were affected by the data breach.

(b) Sensitive financial personal data were involved.

(c) The data breach incident could have been avoided if Toh-Shi had put a better system of checks in place.

(d) Prompt notice was given to the Commission of the data breach incident and Toh-Shi was co-operative during investigation.

(e) Toh-Shi took prompt remedial and preventive actions following the data breach incident.

25 The Commission emphasises that it takes a very serious view of any instance of non-compliance under 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re Spear Security Force Pte Ltd

Case Number: DP-1602-A642
Decision Citation: [2016] SGPDPC 12

Protection Obligation *– Access to personal data – Insufficient administrative and physical security arrangements*

25 July 2016

INTRODUCTION

1 The Personal Data Protection Commission ("Commission") had received a complaint from the Complainant on 24 December 2015 in relation to the lapses by the Respondent's employees in safeguarding the visitor log book of Prive Executive Condominium ("Condominium"), which contained personal data of the visitors. In this regard, the Complainant claimed that the Respondent was in breach of the Personal Data Protection Act 2012[1] ("PDPA").

MATERIAL FACTS AND DOCUMENTS

2 The Complainant was a resident of the Condominium. The Respondent was appointed by the Management Corporation Strata Ttitle of the Condominium to provide security services.

3 According to the Complainant, on several occasions between November 2015 and December 2015, he had observed that the security guards under the Respondent's supervision had left the log book open and unattended on a table near the guard post at the Condominium's entrance.

4 The Complainant further mentioned that he highlighted his concerns to both the Condominium's managing agent and the Respondent but he had not received an adequate response.

1 Act 26 of 2012.

5 In its response to the Commission's investigations into the matter, the Respondent mentioned that it was aware that the visitor log book had been left unattended by its security guards on multiple occasions from the feedback it received, and had taken certain remedial actions since then. These are set out at [7] below.

6 The Respondent further mentioned that the contents of the log book included the visitor's name, mobile phone number, time of entry, the unit number visited and the purpose of the visit. The purpose for the collection of the visitors' details was to ensure that (a) there is no unauthorised entry or trespassing of the premises; and (b) the security guards are able to contact a visitor in the event the visitor has parked in a car park lot that was not allocated to visitors.

7 Following the complaint(s) that was made to the Respondent, the Commission understands that the Respondent had taken remedial actions as follows:

(a) The Respondent had briefed its security guards on the PDPA and put in place certain protective measures such as keeping the log book in the guard post at all times and performing visitor registration there.

(b) The Respondent had also instructed its security guards not to disclose the visitor details to any third parties besides the managing agent and the operations manager of the Condominium.

(c) The security guards were also required to surrender the log book before going for breaks; handing and taking over of the log book between the security supervisors at shift changeovers; and keeping the log book within sight of the security camera.

(d) The Respondent also required security supervisors on duty to remind the security guards prior to every shift on the confidentiality of the visitors' personal data in the log book.

(e) Action may also be taken against the security guards for non-compliance with the Respondent's instructions above – this ranges from progressive warnings to the dismissal of employment.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

8 There is no dispute that the log book contains personal data[2] of the visitors who had visited the Condominimum.

9 Under s 24 of the PDPA, the Respondent is obliged to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, in respect of the personal data contained in the Condominium log book.

10 The Respondent's past practice that was the subject of this complaint was the placement of the visitor log book at a location that was not sufficiently safeguarded from prying eyes nor subject to close supervision by the guards. During the Commission's investigation, the Respondent has not shown that it had put in place any arrangement, or taken any steps, to prevent unauthorised access to the contents in the log book comprising of personal data. On the contrary, given that the log book was left open and unattended on multiple occasions, this allowed for, and increased the opportunities for, unauthorised access to the personal data contained within the log book. The Respondent had only taken action to secure the log book only after it received complaint(s) and/or feedback.

11 Given the lack of any reasonable security arrangement that was in place to prevent the unauthorised access to the personal data in the log book, the Commission finds that the Respondent is in breach of s 24 of the PDPA in respect of the past practice.

ACTIONS TAKEN BY THE COMMISSION

12 Given the Commission's findings that the Respondent is in breach of its obligations under s 24 of the PDPA, the Commission is empowered under s 29 of the PDPA to give the Respondent 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 $1m as the Commission thinks fit.

---

2 Personal data under the Personal Data Protection Act 2012 (Act 26 of 2012) is defined as data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.

13 In considering whether a direction should be made or given to the Respondent in this case, the Commission notes that: (a) while there was a risk of data leakage, there was no evidence suggesting that the visitors' personal data had actually been exposed to unauthorised third parties due to the lapses by the Respondent; and (b) the Respondent had taken reasonably adequate steps to remedy the lapses, as set out above at [7], during the course of the investigations.

14 In view of the factors noted above, the Commission has decided not to impose a financial penalty against the Respondent. Instead, it has decided to issue a Warning against the Respondent for the breach of its obligations under s 24 of the PDPA.

15 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re Chua Yong Boon Justin

Case Number: DP-1411-A247
Decision Citation: [2016] SGPDPC 13

Consent Obligation *– Disclosure of personal data without consent*
Personal or domestic capacity

12 August 2016

INTRODUCTION

1 On 15 November 2014, the Personal Data Protection Commission ("Commission") received an e-mail from the "Complainant" regarding the unauthorised disclosure of personal data of his wife and himself by the property agent of his landlord following a dispute between the Complainant, the Complainant's wife and another tenant, [redacted] ("Ms C"). The Commission proceeded to investigate into the alleged breach of the Personal Data Protection Act 2012[1] ("PDPA"). Its findings into the matter are set out below.

MATERIAL FACTS AND DOCUMENTS

2 The Complainant, his wife and Ms C are tenants of a landed property. For the purposes of entering into the tenancy with the landlord, the Complainant and his wife had previously provided their names and NRIC numbers (amongst other personal data) to the registered salesperson[2] (commonly known as a "property agent") of the landlord, Mr Chua Yong Boon Justin ("Respondent"). The Respondent was registered as a salesperson with Global Property Strategic Alliance Pte Ltd ("GPS"). The Respondent's engagement as a salesperson with GPS was governed by a "Salesperson Agreement" dated 31 October 2011.

1 Act 26 of 2012.
2 Under the Estate Agents Act (Cap 95A, 2011 Rev Ed).

3 In or around November 2014, a dispute arose between Ms C and the Complainant and his wife over the usage of common space within the rented premises, and an argument had apparently ensued between the parties. The Respondent was not present during the argument. However, Ms C had informed him of the argument, and also requested the Respondent to provide her with the names and NRIC numbers of the Complainant and his wife so as to hold the Complainant "responsible" in the event that the Complainant had publicised the photos that were apparently taken in the course of the argument. The Respondent took this to mean that Ms C was prepared to lodge a police report over the matter.

4 The Respondent proceeded to provide Ms C with their full names and NRIC numbers.

5 According to the Complainant, the information was used to send an e-mail to his employer casting allegations against him. There was, however, no proof or evidence of the e-mail that was sent or the impact that the e-mail had on his employment.

6 In response to the Commission's queries on this matter, the Respondent referred to ss 2 and 4(1) of the PDPA, and took the view that he was acting in a "personal or domestic capacity" in the matter, since his actions were unrelated to real estate matters. He also took the view that his "intervention" in the matter was justified in the circumstances.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

7 The main issues that have arisen in this case are as follow:

(a) Was the Respondent acting in a personal or domestic capacity under s 2 of the PDPA?

(b) Did the Respondent comply with his obligations under the PDPA in respect of the disclosure that was made by obtaining consent from the Complainant and his wife for the disclosure?

(c) If not, are any of the exceptions to the PDPA applicable in respect of the disclosure made by the Respondent?

Issue (a): Was the Respondent acting in a personal or domestic capacity under section 2 of the PDPA?

8 Section 4(1)(*a*) of the PDPA carves out an exception in the PDPA for Pts III to VI of the PDPA (*ie*, an exception to the Consent Obligation, the Notification Obligation or the Purpose Limitation Obligation). Section 4(1)(*a*) provides that Pts III to VI of the PDPA shall not impose any obligation on an individual acting in a personal or domestic capacity. The word "domestic" is defined in the PDPA to mean "related to home or family".

9 As mentioned above, the Respondent claimed that he was acting in a personal or domestic capacity when he disclosed the personal data of the Complainant and his wife. If that were the case, he would not need to comply with the relevant provisions of the PDPA (especially the consent and notification provisions)[3] in making the disclosure. It follows that he would not be liable under the PDPA for any omission to carry out any steps or take any action as provided for under Pts III to VI of the PDPA, including obtaining consent from the individual for the disclosure. However, the Commission is of the position that the Respondent cannot rely on s 4(1)(*a*) of the PDPA in this case.

10 In considering the capacity of the Respondent when he disclosed the personal data of the Complainant and his wife, it would be relevant to look at the nature of the relationship between the Respondent, GPS and the landlord, and the context in which the Respondent had dealt with the personal data in question.

11 Under the Salesperson Agreement, it was expressly provided that the Respondent was not a "servant, agent or employee" of GPS. As stated by GPS to the Commission, the Respondent was the one who "represented" the landlord in this case in respect of the transaction for the tenancy. In the Commission's view, the Respondent was carrying out his real estate agency work as a business of his own. Therefore, in dealing with the personal data that the Respondent had collected in the course of his real estate agency work, the Respondent was an "organisation" under the PDPA, separate from the company which had engaged him (*ie*, GPS).

---

3 Under ss 13, 14, 15 and 20 of the Personal Data Protection Act 2012 (Act 26 of 2012).

12 Since the personal data of the Complainant and his wife were collected by the Respondent in the course of his real estate agency work, it was for the Respondent's "business"[4] purposes, and not for his personal or domestic purposes. The Respondent therefore was obliged to comply with the provisions in the PDPA in respect of such personal data that were collected in the course of his work.

13 Accordingly, even if the Respondent had intended to act in a personal or domestic capacity in relation to the dispute that took place between Ms C and the Complainant and his wife, he remains obliged to comply with his obligations under the PDPA. The Respondent cannot take personal data that he had been provided with in his commercial capacity as a registered salesperson and disclose it in a personal or domestic capacity. In other words, the Respondent was not permitted to disclose the personal data as and when he chooses for the reason that he was doing it for "personal or domestic purposes". He was, and remains, obliged to keep that personal data protected pursuant to the provisions of the PDPA.

Issues (b) and (c): Has the Respondent complied with the Consent Obligation under the PDPA or does the disclosure fall under any exceptions under the PDPA?

14 Given, as explained above, that the PDPA continues to apply to the personal data of the Complainant and his wife which were collected by the Respondent, the Respondent is obliged to obtain their consent in order to disclose the personal data to a third party under s 13 of the PDPA, unless an exception applies under the PDPA.

15 Section 13 of the PDPA provides that an organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless (a) the individual gives, or is deemed to have given, his consent under the PDPA to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law. Relatedly, s 14 provides that an individual has not given consent under the PDPA for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless (a) the

4 As defined in the Personal Data Protection Act 2012 (Act 26 of 2012).

individual has been provided with the information required under s 20 of the PDPA; and (b) the individual provided his consent for that purpose in accordance with the PDPA.

16 Based on the facts of this case, the Commission notes that the Respondent had not obtained the consent of the Complainant and his wife for the disclosure of their personal data to Ms C. Accordingly, the Respondent is in breach of s 13 of the PDPA.

17 Additionally, in the Commission's assessment, none of the exceptions under the PDPA would apply to allow the Respondent to disclose the personal data of the Complainant and his wife without consent.

ACTIONS TAKEN BY THE COMMISSION

18 Given the Commission's findings that the Respondent is in breach of his obligations under s 13 of the PDPA, the Commission is empowered under s 29 of the PDPA to give the Respondent 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 $1m as the Commission thinks fit.

19 In this case, the Commission has considered the following pertinent factors:

(a) registered salespersons (as defined under the Estate Agents Act)[5] are likely to collect, receive or obtain a considerable amount of personal data of various individuals (including the personal data of the landlord and the tenants) in the course of their work. It is imperative that these salespersons ensure that the personal data in their possession or control are sufficiently protected, and that they keenly observe the provisions under the PDPA in dealing with the personal data;

(b) in this case, the personal data of two persons were disclosed to a third party without consent or authority; and

(c) it would appear, in this case, that just by the Respondent hearing Ms C's version of events and the accusations made against the Complainant and his wife, the Respondent had, without proper consideration for the personal data which the Respondent was obliged

5 Cap 95A, 2011 Rev Ed.

to protect, released the personal data to Ms C without consent. Given the circumstances in which the personal data were disclosed, the Respondent must have known or would have been aware that there would be repercussions that follow from the disclosure, and that the Complainant and his wife would be affected from the disclosure, now that they can be specifically identified from the information provided. However, the Respondent still proceeded to disclose the personal data of the Complainant and his wife without obtaining consent.

20 Given the considerations set out above, the Commission has decided to impose a financial penalty against the Respondent.

21 On the quantum of the financial penalty, the Commission notes that the Respondent was carrying on his trade independently and, based on what was found above, had failed to fulfil his responsibility of ensuring compliance with the PDPA. However, the Commission also considered that the amount should be set at the lower end of the spectrum given that:

(a) the disclosure had been made to a single individual and it appears to have been done on a one-off instance; and

(b) there was no proof of the impact on the Complainant's employment or the risk of damage or loss in relation to the personal data that were disclosed.

22 In view of the above, a financial penalty of $500 is imposed on the Respondent.

23 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.

LEONG KENG THAI
Chairman
Personal Data Protection Commission

Re Fu Kwee Kitchen Catering Services and another

Case Number: DP-1410-A163
Decision Citation: [2016] SGPDPC 14

Data intermediary *– "Processing" of personal data*
Openness Obligation *– Lack of data protection policies and practices*
Protection Obligation *– Access to personal data – Insufficient technical security arrangements*

21 September 2016

BACKGROUND

1 On 30 September 2014, the Personal Data Protection Commission ("Commission") received a complaint against Fu Kwee Kitchen Catering Services ("Fu Kwee") regarding an alleged data breach by Fu Kwee involving unauthorised access of Fu Kwee's customers' personal data.

2 The Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether there had been a breach by Fu Kwee and/or Pixart Pte Ltd ("Pixart") (the Respondents in this investigation) of their respective obligations under the PDPA.

MATERIAL FACTS AND DOCUMENTS

Fu Kwee's relationship with Pixart

3 Fu Kwee provides food and beverage catering services in Singapore. It owned and managed the following website at the material time of the complaint: <http://www.fukweecatering.sg>, where different customer

1 Act 26 of 2012.

orders could be viewed at the following URLs <http://www.fukweecatering.sg/fixmenu1preview.aspx?pid=[number]>.

4 Pixart is an information technology ("IT") vendor engaged by Fu Kwee in 2010 to (a) develop an online ordering system for Fu Kwee and Fu Kwee's corporate website, and (b) host, support and maintain the website. The PDPA came fully into force on 2 July 2014, and as the contract between Fu Kwee and Pixart was only terminated sometime around April or May 2015, Pixart remained responsible for hosting, supporting and maintaining the website at the time of the alleged data breach incident in September 2014.

Data breach incident

5 The Complainant stated that she was a customer of Fu Kwee, and alleged that she could retrieve another customer's order details and personal data (specifically the customer's name, postal address and personal contact number) by changing the numerals at the end of the URL of Fu Kwee's order preview web page at http://www.fukweecatering.sg/fixmenu1preview.aspx?pid=102 from "102" to "97" from[2] (ie, <http://www.fukweecatering.sa/fixmenu1preview.aspx?pid=97>).

6 At the material time, on 17 September 2014, while Fu Kwee had a default anti-virus programme for its server, it did not implement any measures to protect its customers' personal data from unauthorised access through the type of vulnerability discovered by the Complainant (*ie*, that the personal data of other customers could be viewed by altering the numerals at the end of the URL for Fu Kwee's order preview web page).

7 Fu Kwee appeared to be unaware of this vulnerability until the Commission issued its first Notice to Require Production of Documents and Information under the Ninth Schedule to the PDPA ("NTP") on 12 December 2014. Fu Kwee then instructed Pixart to address the vulnerability on 30 December 2014. No notifications were sent by either Fu Kwee or Pixart to the customers affected by the data breach.

8 Pixart confirmed, from its checks on the system, that the URL of each order preview web page that was generated after a customer's order did not

2 The URL had been taken down shortly after the data breach incident.

expire. Pixart also confirmed that the URL of the order preview web page would include the customer's order ID number, which was as short as three digits and generated sequentially via Fu Kwee's website. This enabled anyone who had a pre-existing URL to access other customers' orders and their personal data simply by altering the numerals at the end of the URL of Fu Kwee's order preview web page.

9 Pixart implemented a "one-time URL" solution on 30 December 2014. This technical solution incorporates a 20-minute exposure security feature that permits a customer to view his or her own order only once before the URL automatically expires after 20 minutes. The URL would also similarly expire if the web page was closed or refreshed by the customer.

10 Investigations revealed that the scope of the contract between Fu Kwee and Pixart did not include the implementation of security measures on Fu Kwee's website to protect customers' personal data. Pixart had also not conducted any penetration tests on Fu Kwee's website. Such penetration tests could have enabled Fu Kwee to discover the design flaw of its order preview web pages.

11 Additionally, in the course of the investigations, Fu Kwee was found not to have implemented any password policy to restrict or control staff access to its database of customers' personal data. Fu Kwee also neither implemented personal data protection policies for the collection, use or disclosure of personal data nor appointed a data protection officer ("DPO") to safeguard its customers' personal data.

12 Having carefully considered the relevant facts and circumstances, including the statements and representations made by Fu Kwee and Pixart, the Commission sets out its findings and assessment herein.

COMMISSION'S FINDINGS AND ASSESSMENT

Issues for determination

13 The issues to be determined in the present case are as follows:

(a) whether Fu Kwee had breached the obligation under s 24 of the PDPA ("Protection Obligation");

(b) whether Fu Kwee had breached the obligation under ss 11 and 12 of the PDPA ("Openness Obligation"), specifically, ss 11(3)

and 12(*a*), for failure to appoint a DPO and put in place privacy policies and practices, in contravention of those sections of the PDPA;

(c) whether Pixart is a data intermediary of Fu Kwee; and

(d) whether Pixart had breached the Protection Obligation.

Issue A: Whether Fu Kwee had breached the Protection Obligation

14 Section 24 of the PDPA states:

> **Protection of Personal Data**
>
> **24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

15 Pursuant to s 24 of the PDPA, Fu Kwee, being an organisation which had its customers' personal data under its possession and/or control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Protection Obligation applies equally to all personal data in the possession or under the control of the organisation, including personal data that the organisation may have collected before 2 July 2014, when the data protection provisions under Pts III to VI of the PDPA came into effect.

16 Following a careful assessment of the relevant facts and circumstances, the Commission is of the view that Fu Kwee had not reasonably discharged its obligation under s 24 of the PDPA until the fixes introduced on 30 December 2014. In particular, the Commission has identified the following vulnerabilities in Fu Kwee's security arrangements, which illustrate how Fu Kwee failed to make reasonable security arrangements to protect customers' personal data:

(a) Fu Kwee's website did not require password access, which could have reasonably restricted unauthorised access to customers' personal data using the website.

(b) The order preview URLs that were generated by Fu Kwee's website whenever a customer placed an order not only did not expire, but were also predictable. This enabled any customer to simply alter the last few digits of an order preview URL in order to access the order details and personal data of other customers.

(c) Fu Kwee acknowledged that it had not instructed Pixart to put in place security measures to protect its customers' personal data even

after 2 July 2014, when the data protection obligations in the PDPA came into force.

(d) The investigations also found that there were no access controls to Fu Kwee's database of customers' personal data. Accordingly, though Fu Kwee had sought to protect its server containing the database using a default Windows firewall, the database remained vulnerable to unauthorised access.

17 The vulnerabilities set out above demonstrate that Fu Kwee could have done more to protect its customers' personal data that was in its possession or under its control. When viewed in totality, the Commission is of the view that Fu Kwee had failed to make reasonable security arrangements to protect its customers' personal data because these vulnerabilities were preventable.

18 Although Fu Kwee had outsourced the hosting, support and maintenance of its online ordering system and corporate website to Pixart (which the Commission has determined to be a data intermediary of Fu Kwee for the reasons set out below), Fu Kwee was ultimately responsible for the security of the website and customers' personal data as if the personal data were processed by Fu Kwee itself (*per* s 4(3) of the PDPA).

19 In light of the foregoing, the Commission finds that Fu Kwee had breached the Protection Obligation at the material time.

Issue B: Whether Fu Kwee had breached the Openness Obligation

20 Sections 11 and 12 of the PDPA together constitute the Openness Obligation under the PDPA, which provides that an organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA, and shall make information about its policies and procedures publicly available. In particular, s 11(3) of the PDPA provides that an organisation shall designate one or more individuals as a DPO to be responsible for ensuring that the organisation complies with the PDPA. In the same vein, s 12(*a*) of the PDPA requires organisations to develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisations under the PDPA.

21 Fu Kwee confirmed that between 2 July 2014 and 12 December 2014, Fu Kwee neither implemented any personal data protection policies for the collection, use or disclosure of personal data, nor appointed a DPO.

22 In light of the foregoing lapses, the Commission finds that Fu Kwee had breached the Openness Obligation.

Issue C: Whether Pixart is a data intermediary of Fu Kwee

23 Under s 2(1) of the PDPA, a "data intermediary" is an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation. The term "processing" in relation to personal data means the carrying out of any operation or set of operations in relation to the personal data and includes, but is not limited to, any of the following: recording; holding; organisation, adaptation or alteration; retrieval; combination; transmission; erasure or destruction. Section 4(2) of the PDPA imposes on a data intermediary the obligation to protect personal data under s 24 of the PDPA and the obligation to cease to retain personal data under s 25 of the PDPA in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. Save for the aforementioned obligations, Pts III to VI of the PDPA do not impose any other obligations on the data intermediary, in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced and made in writing.

24 Based on the facts and representations by Fu Kwee and Pixart, the Commission notes that Pixart was contractually engaged by Fu Kwee in 2010 to (a) develop an online ordering system for Fu Kwee and Fu Kwee's corporate website, and (b) host, support and maintain Fu Kwee's website. As the contract was only terminated sometime in April/May 2015, Pixart was still responsible for hosting, supporting and maintaining Fu Kwee's corporate website and ordering system at the material time of the data breach incident in September 2014.

25 The Commission is of the view that Pixart had processed personal data of Fu Kwee's customers, pursuant to the contract between Fu Kwee and Pixart in relation to the hosting, support and maintenance of the online ordering system and Fu Kwee's corporate website, and Pixart had done so on behalf of and for the purposes of Fu Kwee.

26 In this regard, the Commission finds that Pixart was acting as a data intermediary of Fu Kwee with respect to the relevant websites at the URLs

set out above in connection with the data breach incident, as Pixart essentially processed Fu Kwee's customers' personal data on behalf of and for the purposes of Fu Kwee in hosting, supporting and maintaining the online ordering system and Fu Kwee's website.

Issue D: Whether Pixart had breached the Protection Obligation

27 Section 24 read with s 4(2) of the PDPA imposes a Protection Obligation on data intermediaries in that a data intermediary is obliged to make "reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". In view of the Commission's finding that Pixart was a data intermediary of Fu Kwee at the material time of the data breach incident, Pixart was required to comply with the Protection Obligation under s 24 of the PDPA to protect the personal data it was processing on behalf of and for the purposes of Fu Kwee.

28 In the Commission's view, as a data intermediary, Pixart had an obligation to protect the personal data of Fu Kwee's customers using the ordering system on Fu Kwee's website. Pixart has clearly not discharged the Protection Obligation imposed on it under the PDPA, as it did not have in place reasonable measures to protect the personal data that it was processing for and on behalf of Fu Kwee when it developed, hosted, maintained and provided support in relation to the online ordering system and Fu Kwee's website.

29 In this connection, the Commission notes that if Pixart had advised Fu Kwee on its obligations to protect personal data, but Fu Kwee had rejected Pixart's advice, this could have been taken into account by the Commission as a mitigating factor. However, there is presently no evidence before the Commission suggesting that Pixart had actually advised Fu Kwee on the need to have in place adequate security measures to protect the personal data of Fu Kwee's customers in Fu Kwee's database.

30 In light of the above, the Commission finds that there had been a breach of the Protection Obligation under s 24 of the PDPA by Pixart.

COMMISSION'S DIRECTIONS

31 In assessing the breach and the remedial directions to be imposed, the Commission took into consideration various factors relating to the case, including the mitigating and aggravating factors set out below.

Fu Kwee's breach of the Protection Obligation and the Openness Obligation

32 In relation to Fu Kwee's breach of the Protection Obligation and Openness Obligation, the Commission took into account the following factors:

(a) although Fu Kwee had ample opportunity to put in place reasonable security measures from 2 January 2013 to 2 July 2014, or even after 2 July 2014, when the data protection provisions of the PDPA came into force, it did not do so;

(b) Fu Kwee's disregard for its obligations under the PDPA is also apparent as it had failed to appoint a DPO or put in place policies and practices to comply with the PDPA as at June 2015 (when it appointed a new vendor), even after being notified about the data breach incident in December 2014 by the Commission;

(c) Fu Kwee was not forthcoming in providing information during the investigation, and only provided bare facts in its responses during the investigations; and

(d) notwithstanding that the Commission did not receive any other complaints regarding the relevant websites at the URLs described above, the lapses by Fu Kwee meant that anyone who had the exact URL or who had correctly guessed the parameters could potentially access all the personal data of Fu Kwee's customers who had placed orders online at Fu Kwee's website.

Pixart's breach of the Protection Obligation

33 In relation to Pixart's breach of the Protection Obligation, the following factors were taken into consideration:

(a) Pixart was not forthcoming in providing information during the investigation, and did not respond to the second NTP dated 10 March 2015, which was addressed to Pixart; and

(b) Pixart took active steps to fix the vulnerability in about two weeks after the Commission informed Fu Kwee about the data breach. Based on the Commission's assessment, the remedial actions taken were acceptable.

34 Having completed its investigation and assessment of this matter, the Commission is satisfied that Fu Kwee had been in breach of the Protection Obligation under s 24 of the PDPA, and the Openness Obligation under ss 11(3) and 12(*a*) of the PDPA for the reasons cited above. Pursuant to s 29 of the PDPA, the Commission hereby directs Fu Kwee to do as follows:

(a) pay a financial penalty of $3,000 within 30 days from the date of the Commission's direction;

(b) for all employees of Fu Kwee handling personal data to attend a training course on the obligations under the PDPA and the organisation's data protection policies and practices within six months from the date of the Commission's direction;

(c) conduct a security audit of the website at <http://fukweecatering.com.sg/> to be performed by duly qualified competent contractors or staff. Fu Kwee is to furnish to the Commission, within 30 days from the date of the Commission's direction, a schedule stating the scope of the risks to be assessed and the time within which a full report of the audit can be provided to the Commission, and to confirm in the said report that Fu Kwee no longer stores any personal data of its customers on its website; and

(d) to take steps to appoint a DPO and to develop and implement policies and practices that are necessary for Fu Kwee to comply fully with its obligations under the PDPA, and to provide the Commission with a compliance status update within 30 days from the date of the Commission's direction.

35 The Commission is also satisfied that Pixart has not complied with the Protection Obligation under s 24 of the PDPA for the reasons cited above. Pursuant to s 29(2) of the PDPA, the Commission hereby directs that a financial penalty of $1,000 be meted out against Pixart.

36 The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA and with the Commission's directions. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

LEONG KENG THAI
Chairman
Personal Data Protection Commission

Grounds of Decision

Re Aviva Ltd and another

Case Number: DP-1603-A661
Decision Citation: [2016] SGPDPC 15

Data intermediary *– "Processing" of personal data*
Protection Obligation *– Disclosure of personal data – Insufficient administrative and technical security arrangements*

21 September 2016

BACKGROUND

1 On 9 March 2016, Aviva Ltd ("Aviva") reported to the Personal Data Protection Commission ("Commission") an incident involving the disclosure of the personal data belonging to 7,794 Aviva policyholders under the Aviva Public Officers Group Insurance Scheme ("POGIS"). It was reported that erroneous annual premium statements for the year 2015 had been sent out to the POGIS policyholders. The Monetary Authority of Singapore was also notified of this incident by Aviva on 10 March 2016.

2 On 10 June 2016, Aviva informed the Commission that while 7,794 POGIS policyholders received erroneous annual premium statements for the year 2015, the personal data of a total of 8,022 individuals, including the POGIS policyholders' dependants, were disclosed in the data breach incident.

3 Following the reporting of the incident, the Commission undertook an investigation into the matter. The Commission has determined that the two respondents in this matter are Aviva and Toh-Shi Printing Singapore Pte Ltd ("Toh-Shi"). The Commission's decision on the matter and grounds of decision are set out below.

MATERIAL FACTS AND DOCUMENTS

4 Aviva is an insurance company and the appointed insurer for the POGIS. Toh-Shi provides mail out services of all the correspondence for

Aviva and data printing services for *ad hoc* projects. The mail out and data printing services provided by Toh-Shi to Aviva are governed by a service agreement dated 20 December 2012 as amended by a letter from Aviva to Toh-Shi dated 24 April 2014 and an addendum to the service agreement dated 12 January 2016 ("Addendum" and collectively, the "Toh-Shi Service Agreement").

5 The Toh-Shi Service Agreement provides that, among other things, Toh-Shi shall (a) comply with the Personal Data Protection Act 2012[1] ("PDPA") and all subsidiary legislation related thereto; and (b) have in place an adequate security plan containing Toh-Shi's security policies, procedures and controls in respect of protecting the confidentiality and security of Aviva's information in connection with the provision of the services.

6 During investigations, Aviva represented to the Commission that it has put in place the following security arrangements:

> (a) a Standard Operating Procedure ("SOP") whereby Toh-Shi provides sample cases to Aviva for verification and Aviva is required to sign-off on the sampled cases and give the go-ahead before Toh-Shi can commence printing the finalised documents;
> (b) annual inspections and review of Aviva's arrangement with Toh-Shi are conducted to ensure that Toh-Shi is adhering to its security procedures in handling data, such as data encryption to protect customer data, as well as conducting data sample checks to ensure data consistency and integrity; and
> (c) annual on-site inspections are conducted to verify Toh-Shi's information technology security and business protection measures, and business continuity and disaster recovery capabilities.

7 Similarly, Toh-Shi represented to the Commission that it has a data protection notice (effective 2 July 2014), which sets out the various methods that Toh-Shi has in place to safeguard personal data, and that it has implemented the following security measures and processes:

> (a) Toh-Shi will send user acceptance testing ("UAT") samples to Aviva for Aviva's verification and will only send the processed data for

1 Act 26 of 2012.

printing after Aviva has verified and signed off on the data content form;

(b) Toh-Shi has quality control ("QC") processes in place and conducts sample checks ("QC Sample Checks") to ensure the accuracy of the data printed and that the documents printed match the approved UAT samples;

(c) once the documents are printed, a printout from the mailing machine will record the actual number of letters inserted and this figure will be tallied against the IT report that records the total number of letters computed from the database; and

(d) printing is done in a secured room, with 24/7 CCTV recording. Toh-Shi's data printing supervisor will also observe the operators and ensure that, when verifying the correct positioning of the images and clarity, they do not spend more than the required quick glance (which would afford time for a detailed reading of the printed data).

8 On 8 March 2016, Toh-Shi sent out erroneous annual premium statements ("Erroneous Statements") to 7,794 of Aviva's POGIS policy holders ("Affected POGIS Policyholders"). The Erroneous Statements contained the following information of another POGIS policy holder ("Second Products"):

(a) the name(s) of the other policy holder's dependant(s);
(b) the sum assured under the other policy holder's policy;
(c) the premium amount under the other policy holder's policy; and
(d) the type of coverage under the other policy holder's policy.

9 On the same day, Aviva informed Toh-Shi that three POGIS policyholders had received annual premium statements with Second Products that did not belong to them.

10 After the discovery of the data breach, on 10 March 2016, Aviva and Toh-Shi held a recovery management meeting.

11 On 11 March 2016, Toh-Shi reprinted and sent out the 7,794 corrected statements together with an apology letter prepared by Aviva and a $50 shopping voucher to the Affected POGIS Policyholders. Aviva also gave the Affected POGIS Policyholders a waiver of one month's insurance premium as a token for the inconvenience caused.

12 According to the investigations carried out by Toh-Shi, it was found that the data breach incident had occurred due to an error in the sorting process before the printing of the annual premium statements.

13 In accordance with the usual practice, Aviva had sent the statement details in an Excel file to Toh-Shi for processing, which involved populating the relevant fields in the appropriate document templates. Thereafter, the UAT samples were provided to Aviva and Aviva verified and confirmed that the UAT samples were in order and Toh-Shi could proceed with the printing.

14 However, rather than proceed with the printing of the annual premium statements, Toh-Shi performed further processing by sorting the data according to postal code, overseas address and non-deliverable mail before printing. It did so in order to enjoy postage savings. Toh-Shi did not provide any UAT samples of the further sorted data to Aviva for its verification and confirmation before printing the annual premium statements.

15 Toh-Shi's investigations revealed that the error which resulted in the data breach incident was caused by an incomplete selection of the policyholders' account information in the raw data when Toh-Shi sorted the data further. The annual premium statement can list up to two products depending on the policy that each policyholder is insured. However, due to the incomplete selection of the policyholders' account information by the individual(s) carrying out further sorting, information on the Second Products were excluded and not sorted with the rest of the information which resulted in the information on the Second Products being mismatched.

16 While Toh-Shi had conducted QC Sample Checks, Toh-Shi admitted that the QC Sample Checks failed to spot the error as the QC Sample Checks were verified against the erroneously sorted file instead of the source data from Aviva.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

17 The issues to be determined by the Commission are as follows:

(a) what obligations did Aviva and Toh-Shi each owe under the PDPA in respect of the personal data of the Affected POGIS Policyholders;

(b) did Aviva comply with its obligation under s 24 of the PDPA in respect of the data breach incident that happened; and

(c) did Toh-Shi comply with its obligation under s 24 of the PDPA in respect of the data breach incident that happened.

18 Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks ("Protection Obligation").

19 Under s 2(1) of the PDPA, a "data intermediary" is an organisation which processes personal data on behalf of another organisation but does not include an employee of that organisation. Processing personal data on behalf of another organisation refers to the carrying out of any operation or set of operations in relation to the personal data and includes, but is not limited to, the organisation, adaptation or alternation; retrieval; and transmission of the said personal data.

20 Section 4(2) of the PDPA confers an obligation on the data intermediary to comply with the Protection Obligation and the obligation to cease to retain personal data under ss 24 and 25 of the PDPA respectively.

21 Further, s 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

Relationship between Aviva and Toh-Shi and their obligations under the PDPA

22 Having considered the facts and representations made by Aviva and Toh-Shi, the Commission is satisfied that Toh-Shi was engaged to carry out activities of "processing" personal data on behalf of Aviva as defined in

s 2(1) of the PDPA and was therefore acting as a data intermediary of Aviva.

23 First, while Toh-Shi is not expressly identified as a data intermediary of Aviva in the Toh-Shi Service Agreement, the following extracts from the Toh-Shi Service Agreement show that Aviva had envisaged that Toh-Shi would engage in the "processing" of Aviva policyholders' personal data on its behalf:

> (i) "[Toh-Shi] shall comply with the [PDPA] and all subsidiary legislation related thereto … with regard to *any and all personal data (as defined in the PDPA) that it collects and discloses to and/or receives from Aviva*" [emphasis added]: cl 17.1 of the Toh-Shi Service Agreement as amended by the Addendum; and
>
> (ii) "for any personal data that it collects for or receives from Aviva, [Toh-Shi] shall only process/use such personal data solely for Aviva and in accordance with the instructions/purposes of Aviva or as is necessary for Aviva to fulfil its obligations under the Data Protection Legislation and not disclose such personal data to any other party or insurer" [emphasis added]: cl 17.2(c) of the Toh-Shi Service Agreement as amended by the Addendum.

24 Second, as noted at [13] above, Toh-Shi is responsible for (a) populating in the relevant fields in the appropriate document templates with the raw data received from Aviva, and (b) printing, enveloping and dispatching by post of the finalised annual premium statements on behalf of Aviva.

25 Therefore, the Commission finds that Toh-Shi is a data intermediary of Aviva for the purposes of the PDPA. Pursuant to s 4(2) and s 4(3) of the PDPA, both Aviva and Toh-Shi have an obligation to make reasonable security arrangements to protect the personal data of the Aviva policyholders.

Whether Aviva has complied with its obligations under section 24 of the PDPA

26 Based on the Commission's investigation into the matter, it is satisfied that Aviva has met its Protection Obligation under s 24 of the PDPA as it has made reasonable security arrangements to protect the personal data in its possession or under its control.

27 As noted at [6] and [7] above, the Toh-Shi Service Agreement required Toh-Shi to put in place adequate security policies, procedures and controls to protect the confidentiality and security of the Aviva policyholders. The Commission is also satisfied that Aviva has demonstrated that it has undertaken an appropriate level of due diligence to assure itself that its data intermediary, Toh-Shi, is capable of complying with the PDPA. Having done so, it was reasonable for Aviva to have expected Toh-Shi to take the necessary actions to protect the Affected POGIS Policyholders' personal data. Additionally, Aviva had no direct part to play in the actual breach itself, given that the data breach was mainly caused by Toh-Shi's staff failing to comply with its own security measures and procedures, as will be elaborated upon below.

28 Therefore, the Commission does not find Aviva to be in breach of s 24 of the PDPA.

Whether Toh-Shi has complied with its obligations under section 24 of the PDPA

29 Having considered the facts and representations made by Toh-Shi and Aviva, the Commission is of the view that Toh-Shi had failed to take reasonable security measures to protect the personal data it processed on behalf of Aviva.

30 As stated at [7] above, the Commission notes that Toh-Shi did have in place some security arrangements and procedures to safeguard the personal data that Toh-Shi processes on behalf of Aviva.

31 However, despite the fact that Toh-Shi had implemented security arrangements and procedures, Toh-Shi does not dispute that the data breach incident occurred as a result of:

> (a) an error that occurred when Toh-Shi carried out further sorting of the data that had already been verified and confirmed by Aviva (*viz*, sorting by postal code, overseas address and non-deliverable mails);
> (b) Toh-Shi's deviation from the SOP when it did not provide the UAT samples of the data that had undergone further sorting to Aviva for verification and confirmation before printing the finalised annual premium statements; and
> (c) mistakes by the individual(s) conducting the QC Sample Checks in failing to verify the data that had undergone further sorting against

the source data file provided by Aviva (but against the erroneously sorted file prepared by Toh-Shi).

32 Toh-Shi also represented that it has taken the following remedial steps following the data breach incident:

(a) remind and retrain its staff to be more vigilant in processing the customer's data;

(b) ensure that Toh-Shi staff follow the customer's SOPs including any new SOPs to enhance data processing and not deviate from it unless it has been approved by the customer; and

(c) remind Toh-Shi staff that all final products must be approved by the customer before mailing out and not to alter the data after Toh-Shi has obtained the customer's confirmation.

33 Notwithstanding the security measures and procedures implemented by Toh-Shi to protect the very sensitive financial data it processed on behalf of Aviva, the Commission notes that Toh-Shi itself admitted that the data breach incident was caused by errors that occurred because its staff had failed to comply with the company's own security measures and procedures.

34 In the Commission's view, the error in the further sorting process could have been avoided and the data breach incident could have been prevented if:

(a) Toh-Shi had provided samples to Aviva for further verification after sorting; and

(b) Toh-Shi had conducted its QC Sample Checks on the further sorted data against the original source data from Aviva.

35 As such, in view of all of the relevant facts and circumstances, the Commission is not satisfied that Toh-Shi has made reasonable security arrangements to prevent authorised access, collection, use, disclosure, copying, modification, disposal or similar risks in compliance with the Protection Obligation under s 24 of the PDPA.

ENFORCEMENT ACTION TAKEN AGAINST TOH-SHI

36 Having completed its investigation and assessment of this matter, the Commission finds that Aviva is not in breach of s 24 of the PDPA. However, the Commission finds that Toh-Shi is in breach of s 24 of the PDPA.

37 In exercise of the power conferred upon the Commission pursuant to s 29 of the PDPA, the Commission directs that a financial penalty of $25,000 be imposed on Toh-Shi.

38 In assessing the breach and the directions to be imposed, the Commission took into account the following factors:

(a) a large number of individuals (totalling 8,022, including the Affected POGIS Policyholders' dependants whose personal data were disclosed in the data breach incident) were affected by the data breach;

(b) the personal data disclosed in the data breach, namely, the names of the policyholder's dependants or beneficiaries, the sum insured under the insurance policy, the premium amount and type of coverage, are of a sensitive nature, not merely from a financial perspective but can also be socially embarrassing;

(c) this is the second time in a short span of approximately one year that Toh-Shi has committed a breach of s 24 of the PDPA and both of the data breach incidents involve similar fact patterns and causes:

(i) in Toh-Shi's first breach of s 24 of the PDPA[2] in June 2015, erroneous account statements were sent to 195 Central Depository ("CDP") account holders ("First Breach"). The Commission found that the cause of the First Breach was due to errors made by Toh-Shi staff during the printing process, such as a misalignment of the pages during the sorting process which led to errors in the compilation of multi-page CDP statements. A financial penalty of $5,000 was imposed on Toh-Shi in the First Breach; and

(ii) despite the fact that Toh-Shi had taken steps to improve on the security of its system following the First Breach, a similar error in the sorting process has recurred in the present case within a year of the First Breach, which suggests that there is still a weakness in Toh-Shi's internal work processes;

(d) the data breach could have been avoided if Toh-Shi had followed the established SOP. Since Toh-Shi had performed additional sorting, the QC Sample Checks ought to have been carried out again;

---

2 The Commission's decision in *Central Depository (Pte) Limited and Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC 11.

(e) prompt notice was given to the Commission of the data breach incident; and

(f) Toh-Shi was co-operative during the investigation and took prompt remedial and preventive actions.

39 The Commission emphasises that it takes a very serious view of any instance of non-compliance under 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.

LEONG KENG THAI
Chairman
Personal Data Protection Commission

Grounds of Decision

Re ABR Holdings Limited

Case Number: DP-1408-A030
Decision Citation: [2016] SGPDPC 16

Protection Obligation *– Access to personal data – Insufficient technical security arrangements*

23 September 2016

BACKGROUND

1 On 18 March 2014, the Complainant informed the Personal Data Protection Commission ("Commission") that by entering either:

(a) a random 8-digit number as a simulated membership number; or

(b)a simulated unique identification number ("UIN") number (*eg*, NRIC or birth certificate number with a valid check digit),

on the Respondent's Swensen's Kids' Club website, <http://swensens.prism 4u.com> ("Website"), one could access a Swensen's Kids' Club member account associated with that membership or UIN number. Once accessed, the member's name and date of birth ("DOB") would be shown.

2 The provisions in the Personal Data Protection Act 2012[1] ("PDPA") relating to the protection of personal data were not in force at the time of the complaint. The Commission wrote to the Respondent on 2 April 2014 to notify the Respondent of the complaint and that the provisions relating to protection of personal data would come into force on 2 July 2014.

3 On 15 July 2014, the Complainant submitted a further complaint claiming that on that date, the Respondent's Website still allowed access to a member's name and DOB by entering either a simulated membership number or valid UIN number.

1 Act 26 of 2012.

4 On account of the complaints made, the Commission commenced an investigation under s 50 of the PDPA to ascertain whether the Respondent had breached its obligations under the PDPA. The material facts of the case are as follows.

MATERIAL FACTS AND DOCUMENTS

5 The Respondent has been operating the Swensen's chain of restaurants since 1978. The Swensen's Kids' Club is a membership programme which the Respondent runs for children between four and 12 years of age. By accumulating a certain number of electronic "stamps", Swensen's Kids' Club members may be eligible for various promotional offers from the Swensen's chain of restaurants (*eg*, a free Kids' Club Sundae every month with dine-in food order). Each member would be assigned an 8-digit membership number by the Respondent. Membership numbers run sequentially.

6 The Website supports the Swensen's Kids' Club membership programme and allows a member to access information relating to his membership account. The Website has been in operation since 2013 and is maintained and operated by the Respondent's vendor, Prism4u (Singapore).

7 As part of the investigation, the Commission verified that access can be obtained to a member account on the Website by (a) entering a random number sequence simulating a valid membership number; or (b) entering a valid UIN number in the form of a birth certificate number. The Website did not require any password to be entered nor authentication in any other form before granting access.

8 The following details about a member were made available through the Website:

(a) name;
(b) DOB;
(c) redemption status of Kids' Club Sundaes and "stamps";
(d) number of "stamps" accumulated; and
(e) membership expiry date.

9 The Respondent was notified of the further complaint by the Commission on 5 August 2014.

10 On the same day, the Respondent made changes to the Website to remove the display of the member's name and DOB. The effect of the changes were such that when the account is accessed using either a valid membership number or valid UIN number, the only details available would be information concerning redemption status, the number of "stamps" accumulated and the membership expiry date.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Issue to be determined

11 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

12 The issue in the present case is whether the Respondent had breached s 24 of the PDPA (during the period between 15 July 2014 and 5 Aug 2014), when personal data (of members of the Swensen's Kids' Club) could be accessed on the Website (in the manner described at [7] and [8] above).

Whether Respondent had complied with section 24

13 The personal data accessible on the Website included the name and DOB of members of the Swensen's Kids' Club. The names of the members fall within the definition of "personal data" under the PDPA.

14 The personal data accessible on the Website were also under the control of the Respondent. The Respondent demonstrated this control when it was able to promptly effect changes to the Website to block access to such personal data when contacted by the Commission.

15 The Respondent's system allowed the use of either (a) the membership number assigned to each member, or (b) the UIN number of the member, to serve the separate functions of identification of member and authentication to access personal data. These numbers were therefore the only security arrangement put in place by the Respondent to protect personal data on the Website.

16 In the Commission's view, where a single string of numbers is the only security arrangement serving both to identify and authenticate access to personal data, the numbers can possibly constitute reasonable security arrangements depending on the sensitivity of the personal data being protected, and only if this number was unique, unpredictable and reasonably well protected.

17 In this case, the Respondent's use of membership numbers or UIN numbers did not constitute reasonable or adequate security arrangements for the personal data in its possession or under its control because:

(a) the membership numbers assigned by the Respondent to its members were issued in running sequence. The Complainant was able to easily ascertain the number of characters required for a valid membership number and deduce another member's membership number since they were issued sequentially. Tools that are able to generate number sequences, which can be entered as membership numbers, are also readily available online making it relatively easy to simulate other membership numbers;

(b) tools are readily available online that can simulate or generate UIN numbers (such as NRIC and birth certificate numbers); and

(c) once a generated membership or UIN number coincided with an assigned membership number or a member's UIN number, unauthorised access to the member's account and his personal data was possible. Until the system was altered to display only the accumulated "stamps", expiry date and redemption status, the child's name and date of birth were also displayed.

18 In view of the above, the Commission finds that the Respondent had failed to make reasonable security arrangements to protect personal data in its possession or under its control in the period between the commencement of the PDPA on 2 July 2014 and 5 August 2014, when the Commission notified the Respondent a second time regarding the same vulnerability. As such, the Respondent was in breach of s 24 of the PDPA.

ACTIONS TAKEN BY THE COMMISSION

19 Given the Commission's findings that the Respondent is in breach of its obligations under s 24 of the PDPA, the Commission is empowered

under s 29 of the PDPA to issue the Respondent 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 $1m.

20 In determining the direction, if any, to be made, the Commission considered the following factors:

(a) the Respondent was first notified of the vulnerability on 2 April 2014, before the PDPA came into force, thereby giving it ample time to take corrective measures;

(b) this infraction took place during the first month that the PDPA took effect;

(c) the personal data that was disclosed was largely limited to members' names and DOBs; and

(d) the Respondent took prompt action to remedy the breach within the same day when notified by the Commission a second time on 5 August 2014.

21 In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning to the Respondent for the breach of its obligations under s 24 of the PDPA.

22 The Commission 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.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re Comfort Transportation Pte Ltd and another

Case Number: DP-1408-A054
Decision Citation: [2016] SGPDPC 17

"Business contact information"
Continued use of personal data after appointed day

23 September 2016

BACKGROUND

1 On 15 August 2014 and 22 August 2014, the Personal Data Protection Commission ("Commission") received complaints from [redacted] ("First Complainant") and [redacted] ("Second Complainant") against Comfort Transportation Pte Ltd ("First Respondent") and CityCab Pte Ltd ("Second Respondent") respectively for disclosing their personal mobile phone numbers to customers who booked the taxis driven by them.

2 Pursuant to s 50 of the Personal Data Protection Act 2012[1] ("PDPA"), the Commission carried out an investigation into the matter.

MATERIAL FACTS AND DOCUMENTS

3 The First and Second Respondents (collectively, the "Respondents"), are companies within a group that operate a taxi business. Commencing some time in 2013, the Respondents provided a mobile application ("the App") that allowed passengers to make current or advance bookings. The App is owned by the First Respondent. Upon booking a taxi through the App, the mobile phone number of the taxi driver will be sent to the booking passenger's mobile phone together with a confirmation of the taxi booking.

1 Act 26 of 2012.

4 The Complainants, in separate complaints alleged that their mobile numbers are their personal data, and the Respondents are obliged to protect such data in accordance with the PDPA. The First Complainant, in particular, asserted that the First Respondent is not permitted to disclose his mobile number to the booking customers without his consent. The First Complainant claimed that he did not provide such consent to the First Respondent.

5 The Commission understands that the mobile phone numbers that were disclosed were obtained from the Hirer Application form and/or New Relief Application Form (collectively, the "Application Forms") for the hire of a taxi submitted by new drivers. At the material time when the Respondents' mobile phone numbers were collected from them, the App had not been introduced and there is therefore no question that consent to disclose their mobile phone numbers through the App could have been obtained from them.

6 The practice of giving passengers the mobile phone number of drivers who accepted their advance bookings started in September 2013 and was extended to current bookings in July 2014:

(a) On 23 September 2013, the Respondents, in a joint circular, informed their taxi drivers of the initiative to release to passengers the mobile phone numbers of drivers who have accepted their advance bookings.

(b) On 9 July 2014, the Respondents, again in another joint circular, informed their taxi drivers of the initiative to extend the release of the mobile phone numbers of the driver to passengers who have made current bookings.

7 Further, when a driver's bid for an advance or current booking is successful, the taxi's in-vehicle mobile data terminals ("MDT") would show a message prompt containing an "OK" button and a note at the bottom that the driver's personal mobile phone number will be released to the passenger for "ease of communication".

COMMISSION'S FINDINGS AND ASSESSMENT

8 The nature of the relationship between the Complainants and the Respondents is central to understanding how the mobile phone number ought to be treated. Based on the information and documents obtained in

the investigation, the Commission concludes that the taxi drivers of the Respondents (which includes both Complainants in this matter) were not employees of the Respondents, but were independent hirers plying their trade as taxi drivers on their own account, for the following reasons:

> (a) the business of a taxi driver falls under the definition of "business" under s 2(1) of the Business Registration Act[2] ("BRA") read with the First Schedule to the BRA. This means the business of a taxi driver is recognised as a business (as opposed to a form of employment), albeit it is a business that is exempt from registration under the BRA;
>
> (b) the taxi hiring agreement and the terms and conditions issued by the Respondents identify their taxi drivers as "hirers". This evinces the intention that the relationship that the Respondents intended to have with the Complainants was that of a contract to lease a motor vehicle intended to be used by the Complainants to carry on their business as taxi drivers; and
>
> (c) crucially, the taxi fare was not collected on behalf of nor paid to the Respondents, but paid to and kept by the Complainants *in toto*. The Respondents are paid, and only receive, the hiring charges of the taxis from the Complainants.

9 In view of the foregoing, the Commission concludes that the taxi service provided by the taxi drivers of the Respondents falls within the definition of a "business" under s 2(1) of the PDPA. This means that the mobile phone numbers that are used for, or relate to, the business can potentially fall within the definition of "business contact information", and hence be exempted from Pts III to IV of the PDPA (*ie*, the main data protection provisions).

10 The relevant provision exempting the application of Pts III to IV of the PDPA to "business contact information" is found at s 4(5) of the PDPA. "Business contact information" has been defined in the PDPA to mean "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".[3] There is

2 Cap 32, 2004 Rev Ed.

3 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

nothing in this definition that prevents a mobile phone number from use as a "business telephone number", nor is it desirable to exclude mobile phone numbers from the scope of this term since many businesses and individuals provide their mobile phone numbers in the course of their trade or business.

11 The more fundamental question is whether the Complainants' mobile phone numbers can be business contact information when, at the time that they were collected and used, there was no legal concept of "personal data" nor the distinction between "personal data" and "business contact information", since the PDPA had not been enacted. The PDPA has retrospective effect pursuant to s 19 of the PDPA, which applies to personal data collected before its enactment and used for a consistent purpose after its entry into force. To give full effect to the PDPA, particularly when it is applied to personal data collected before its entry into force and that continues to be used for a consistent purpose thereafter, it is necessary to adopt a sensible and pragmatic approach. If the *conduct* of the parties at all material times discloses an *intention* to treat the disclosure and use of the Complainants' mobile phone numbers as disclosure and use for the purpose of their *business* as taxi drivers, the conclusion must naturally be that these were business telephone numbers within the meaning of business contact information; notwithstanding that the legal concept did not exist before the enactment of the PDPA.

12 Having considered the facts of this case, the Commission concludes that the mobile phone numbers were, at the material time, disclosed and used as business telephone numbers and, accordingly, are the business contact information of the taxi drivers; thereby exempting the Respondents from complying with Pts III to IV of the PDPA in respect of the mobile phone numbers. The reasons and considerations for this conclusion are summarised as follows.

13 First, the mobile phone numbers of the Complainants were collected when they applied to hire a taxi from the Respondents. As discussed above, the nature of the relationship between the Complainants and Respondents was commercial as between lessors of taxis and sole proprietors carrying on the business of taxi driving.

14 Second, commencing September 2013, the mobile phone numbers were used by both parties for the purpose of the Complainants' business as taxi drivers when the Respondents started to disclose the mobile phone

numbers to passengers as a means of contacting the taxi driver for advance bookings. In this regard, it also bears noting the following facts, highlighted above:

(a) the Complainants were specifically informed that the mobile numbers of the taxi drivers would be disclosed to passengers who have accepted their advance bookings. Likewise, the taxi drivers would receive a prompt on the MDT informing taxi drivers that their mobile numbers would be released to passengers; and

(b) none of the Complainants had challenged or objected to this practice or to their mobile numbers being disclosed to passengers who made the advance bookings in that period of time.

15 Third, the practice of disclosing the Complainants' mobile phone numbers to passengers for advance bookings was extended to current bookings from July 2014. The conduct of the Respondents was consistent as the extension was for the same purpose as before, *viz*, to provide passengers a means of contacting the taxi drivers. This provides passengers with a consistent level of service for both advance and current bookings. It was a natural and foreseeable extension as the means of direct communications between taxi driver and passenger with a booking is necessary and desirable, whether the booking is made in advance or otherwise.

16 Fourth, the provision of direct means of communications between taxi driver and passenger with a booking is consistent with the nature of the commercial relationship between Complainants and Respondents. After taxi driver and passenger are matched through the booking service, the Respondents have no ability to control the Complainants as they are not employees. Since each taxi driver plies his trade on his own account, driver and passenger should therefore communicate directly for matters concerning the delivery of the taxi service, *eg*, clarifying the precise location for embarkation, delays in pick up or arrival at pick up location, cancellation of booking, *etc*.

17 It is therefore clear to the Commission that the mobile phone numbers were used as business telephone numbers and therefore are in the nature of business contact information. Since the Complainants' mobile phone numbers are business contact information for the purposes of the PDPA, the Respondents are not bound by the provisions in Pts III to VI of the PDPA in respect of the disclosure of the taxi drivers' mobile numbers to

booking customers, in particular, the need to obtain the taxi drivers' consent prior to disclosing the mobile numbers under ss 13, 14, 15 and 20 of the PDPA. In the premises, the alleged acts or omissions complained of by the Complainants do not amount to breaches under the PDPA.

18 For the reasons set out above, the Commission found that the Respondents have not contravened the PDPA, and decided to take no further action on the complaints made under the PDPA.

YEONG ZEE KIN
Commission Member
Personal Data Protection Commission

Grounds of Decision

Re GMM Technoworld Pte Ltd

Case Number: DP-1603-A656
Decision Citation: [2016] SGPDPC 18

Protection Obligation *– Disclosure of personal data – Insufficient technical security arrangements*

30 September 2016

BACKGROUND

1 GMM Technoworld Pte Ltd ("Respondent") is a small and medium enterprise ("SME") retailing products such as waterproof gadgets and measuring instruments. In particular, the Respondent is the sole distributor of DiCAPac, a brand of waterproof cases for cameras and mobile phones.

2 On 3 March 2016, the Personal Data Protection Commission ("Commission") received a complaint from a member of the public regarding the alleged disclosure of personal data on the Respondent's corporate website at <http://www.dicapac.com.sg/frm_display/product-warranty-registration/> ("Web Page").

3 The Commission decided to carry out an investigation into the matter and its findings are set out below.

MATERIAL FACTS AND DOCUMENTS

4 The Respondent created a corporate website (<www.dicapac.com.sg>) on a WordPress platform for the purpose of marketing its products. The website was hosted on a third-party server and comprised several publicly accessible web pages. In 2014, the Respondent added a product warranty registration feature to the website at <http://www.dicapac.com.sg/product-warranty-registration-form/> ("Warranty tab").

5 The Warranty tab contained an online warranty registration form ("Form") for customers who purchased a DiCAPac waterproof case to register for the product warranty. This Form was created using Formidable

Forms, a third-party paid plug-in for WordPress, which allowed for the capture of personal data on the website ("Plug-in"). The information to be provided in the Form included the customers' names, e-mail addresses, mobile phone numbers and residential addresses.

6 The Plug-in had the function of dynamically listing and displaying on the Web Page the personal data that were collected on the website via the Plug-in. According to the Respondent, it was unaware of this function of the Plug-in, and had thought that the personal data that were collected were only viewable by the administrator of the website. As a result of the Respondent's misunderstanding of the functionality of the Plug-in and the (incorrect) use of the Plug-in, the personal data of approximately 190 individuals collected through the Plug-in were displayed on the Web Page, which was publicly accessible on the Internet.

7 After being notified of the breach, the Respondent undertook certain corrective actions to rectify the unauthorised disclosure.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Relevant issue in this case

8 Section 24 of the Personal Data Protection Act 2012[1] ("PDPA") states that an organisation is obliged to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised disclosure, disposal, access, collection, use or similar risks (amongst others).

9 The relevant issue in this case is whether the Respondent had in place reasonable security arrangements to protect the personal data in its possession or in its control, as required under s 24 of the PDPA.

Commission's findings on the relevant issue

10 In this case, the Commission found that the Respondent was ignorant of or unaware that one of the functions of the Plug-in was to display the

1 Act 26 of 2012.

personal data collected on the website. Further, the Commission found no reasonable excuse for the Respondent's ignorance for the following reasons.

11 First, the Plug-in was promoted on the Formidable Forms website with the following description indicative of its functions "[d]on't just collect information, display it".[2] Second, the product documentation web page contained the following statement: "[a]ny data entered into a Formidable Form can be displayed on your site using Views".[3] On the same web page, one of the display options under the heading "View Format" was "All Entries", which was described as an option that would "[l]ist all entries from the specified form".[4] Third, the Formidable Forms website had a "demos" web page that allowed users to try out or download a demonstration of how the information captured by the Plug-in would be displayed. In gist, a dominant feature of the Plug-in is that it provided online form functionalities for the collection *and display* of information on the website.

12 In this regard, the Formidable Forms website had web pages which provided adequate demonstrations, documentation and explanations of its products, including the Plug-in, accompanied by pictorial guides. In the Commission's view, an organisation ought to have sufficient understanding and appreciation of a product before making use of it. In this case, had the organisation studied these sources, it would have become aware that use of the Plug-in would result in the disclosure of the data collected on the website since the Plug-in was designed to ease the collection and display of information. For the organisation's purpose of collecting but not displaying personal data, the default behaviour of the out-of-the-box features of this Plug-in would not be appropriate. Alternatives could have been considered. If alternatives are not suitable and the organisation decides to proceed with using the Plug-in, it should be responsible for understanding the security features offered by the Plug-in and it would have to set the security features accordingly. It would not be prudent for an organisation to use a plug-in without first being clear of the default behaviour of its functions in relation

2 Excerpt from Formidable Forms website (<https://formidablepro.com/>).

3 Excerpt from Documentation of Formidable Forms "View Settings" (<https://formidablepro.com/knowledgebase/display-your-form-data/>).

4 Excerpt from Documentation of Formidable Forms "View Settings" (<https://formidablepro.com/knowledgebase/display-your-form-data/>).

to the collection of personal data, and without ensuring that the plug-in (if properly configured) adequately protects the organisation's personal data.

13 For completeness, investigations revealed that the Respondent did not mention taking any further steps to protect the personal data in its possession or under its control. Instead, the Respondent appears to have relied on the belief that the paid Plug-in itself was sufficiently secure out-of-the-box.

14 Ultimately, the Respondent's lack of awareness of the Plug-in's actual functions, its wrong use of the Plug-in, and failure to take steps to configure it appropriately led to the unauthorised disclosure of the personal data of approximately 190 individuals. Accordingly, this was a breach of s 24 of the PDPA.

COMMISSION'S DIRECTIONS

15 The Commission is empowered under s 29 of the PDPA to give the Respondent such directions as it deems fit to ensure the Respondent's compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding $1m as the Commission thinks fit.

16 In determining whether a direction should be given to the Respondent in this case, the Commission has given due consideration to all the relevant factors, including the following:

(a) the Respondent was co-operative and provided its responses to the Commission on a timely basis; and

(b) the Respondent took immediate steps to stop the further unauthorised disclosure, and implemented corrective measures to protect its customers' personal data.

17 Pursuant to s 29(2) of the PDPA, and having completed its investigation and assessment of this matter, the Commission is satisfied that the Respondent was in breach of the protection obligation under s 24 of the PDPA.

18 Having carefully considered all the relevant factors of this case, the Commission hereby directs the Respondent to pay a financial penalty of $3,000 within 30 days from the date of the Commission's direction, failing

which interest shall be payable on the outstanding amount of such financial penalty.

19 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.

LEONG KENG THAI
Chairman
Personal Data Protection Commission

Grounds of Decision

Re Smiling Orchid (S) Pte Ltd and others

Case Number: DP-1411-A250
Decision Citation: [2016] SGPDPC 19

Data intermediary *– Obligations of organisation and data intermediary*
Data intermediary *– Whether an organisation is a data intermediary*
Protection Obligation *– Access to personal data – Insufficient technical security arrangements*

4 November 2016

BACKGROUND

1 On 24 November 2014, the Personal Data Protection Commission ("Commission") received a complaint from the Complainant, Mr X, in relation to the failure of the first Respondent, Smiling Orchid (S) Pte Ltd ("Smiling Orchid"), a food caterer, to put in place reasonable security measures on its website to prevent disclosure of their customers' personal data.

2 Following the Complainant's complaint, the Commission undertook an investigation into the matter. The Commission has determined that there are four Respondents in this matter, namely:

(a) Smiling Orchid;
(b) T2 Web Pte Ltd ("T2");
(c) Cybersite Services Pte Ltd ("Cybersite"); and
(d) East Wind Solutions Pte Ltd ("East Wind").

3 The Commission's decision on the matter and grounds of decision are set out below.

MATERIAL FACTS AND DOCUMENTS

4 Smiling Orchid is a food catering company.

5 Smiling Orchid owns the rights to two different domains, namely, <smilingorchid.com> and <smilingorchid.com.sg>. Customers can place orders for Smiling Orchid's bakery and catering services through its website.

6 T2 is a web design and development company. By way of a project agreement between T2 and Smiling Orchid dated 29 July 2008 ("Project Agreement"), T2 was engaged by Smiling Orchid to design the Smiling Orchid web page and build a content management system ("CMS") to manage Smiling Orchid's bakery and catering content on its website.

7 T2 created the design and HTML code but outsourced the development of the entire CMS to a freelancer, who in turn subcontracted the actual development of the CMS to another entity that T2 has only identified as "developers based in China". T2 represented that there are no records available about (a) how the CMS was tested by the developer; or (b) systematic acceptance tests done by the respective contractor.

8 Cybersite was the domain and website hosting provider for Smiling Orchid from 3 April 2014 to 3 April 2016 and had, in its possession, the personal data of Smiling Orchid's customers stored on its servers in Singapore. Since 24 April 2015, Smiling Orchid has changed its hosting providers and T2 has been hosting Smiling Orchid's website via Pozhub Solutions Pte Ltd ("Pozhub Solutions"), but Cybersite continued to host the domain name.

9 East Wind is the new information technology ("IT") service provider to Smiling Orchid that was engaged after the occurrence of the data breach complained of by the Complainant to help Smiling Orchid with ensuring basic security and prevention for its portal and infrastructure.

10 On 1 August 2014, the Complainant placed an order on Smiling Orchid's website for a workplace event on 28 August 2014 ("Order").

11 On or around 10 November 2014, the Complainant did a random search of his full name on <www.yahoo.com.sg>. Among the search results was a URL link to a website containing details of the Complainant's Order, including his full name, residential address, mobile number, workplace address and workplace e-mail address ("Data Breach Incident").

12 On 11 and 18 November 2014, the Complainant reported the Data Breach Incident to Smiling Orchid but did not receive any response. Thereafter, the Complainant lodged a complaint with the Commission.

13 Based on the Commission's investigation into the matter, the Commission also found that as at 18 February 2015, the preview order function at the URL <http://www.smilingorchid.com/admin/orde/catering/cateringOrderDetail.php?pkid=5893> displayed the order details of other Smiling Orchid customers and that by changing the numerals at the end of the URL, the order details of other customers could be accessed.

14 In November 2015, the Commission noted that the order information was again accessible on Smiling Orchid's website without authentication. In fact, not only could the direct link be used as before, the following alternative link yielded a whole list of orders, which could be accessed from the hyperlinks within that list: <http://www.smilingorchid.com/admin/order/catering/cateringOrderList.php>.

15 It is not disputed that the details of the customers' orders contained personal data under the control of Smiling Orchid at the material time.

How the Data Breach Incident occurred

16 In its responses to the Commission during the investigation, Smiling Orchid represented that it was only made aware of the Data Breach Incident and the security vulnerability when the Commission informed it of the investigation arising from the Complainant's complaint.

17 Smiling Orchid represented that it had depended on T2 to be "in charge of the site" and had expected that T2 would highlight any security issues that Smiling Orchid should have paid attention to. This was despite the fact that (a) the security of the site or the CMS was not included under T2's scope of work under the Project Agreement; (b) Smiling Orchid conceded that issues of security did not cross their mind and T2 was engaged mainly to enhance the design of their website; and (c) Smiling Orchid did not recall discussing any aspects of website security with T2.

18 In turn, T2 denied that it was responsible for Smiling Orchid's website security at the time of the Data Breach Incident and alleged that Cybersite was the party in charge of Smiling Orchid's website security.

19 Cybersite admitted that it was responsible for the security of the hosting system. Cybersite represented that it had employed a basic hosting model using shared services, provided regular security updates of basic hosting provisions such as firewall, anti-virus and anti-spam software and regularly changed the system password as part of its security process.

However, Cybersite conceded that it did not conduct regular security testing such as an intrusion test as part of its processes.

20 T2 represented that upon being informed by Smiling Orchid in February 2015 of the Data Breach Incident, T2 conducted investigations and discovered that the code protecting the site content had been removed. As a result, data which were supposed to be protected and accessible only by users with administrator rights could be accessed by users without such administrator rights. In response, T2 changed the administrator and server passwords and added back the lines of code protecting the site content.

21 T2 also represented that there may have been similar instances where the administrator rights were removed but T2 was not able to provide details of when such incidents occurred. Whenever such an incident occurred, T2 would change the administrator and server passwords, and check and reinstate the codes to secure the website.

22 T2 hypothesised that the Data Breach Incident may have been caused by the following: (a) that hackers compromised the security of the administrator module notwithstanding the existence of the password protection; or (b) that Smiling Orchid's employees had shared their passwords to the website.

23 With regard to T2's first hypothesis, T2 represented that the CMS was assumed to be designed in such a way that normal usage of the CMS by staff would not result in changes to the code. The code was intended to be static to such users. However, T2 conceded that as the development of the CMS was outsourced, no test records were available and it did not know how extensively this function had been tested by the developers or contractors.

24 Investigations carried out by Cybersite and the new hosting provider, Pozhub Solutions, disclosed no record of any cyber-attacks to its hosting system for Smiling Orchid between June 2014 and November 2014 when the Data Breach Incident had occurred.

25 In relation to T2's second hypothesis, T2 represented that the administrator password was known to T2, one of the freelancers and to a few people within Smiling Orchid, one of whom has since left Smiling Orchid. Any one of these persons could have created new administrator accounts and passwords. There were no logs that can conclusively rule out this possibility.

26 T2 conceded that there was no known enforcement of password strength or password length within the system. In fact, T2 represented that the password was "likely" part of the PHP framework configuration file and was likely stored in clear text. If not, it would be part of the MySQL database. T2 admitted that it had seen and removed some passwords within the MySQL database.

27 To date, the root cause of the recurring removal of the code which allowed access to the personal data on the database without the administrator password has not been ascertained.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

28 The issues to be determined by the Commission are as follows:

(a) what obligations did each of the Respondents owe under the Personal Data Protection Act 2012[1] ("PDPA") in respect of the Complainant's personal data; and

(b) did each of the Respondents comply with its obligation under s 24 of the PDPA in respect of the Data Breach Incident.

29 Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks ("Protection Obligation").

30 Section 2(1) of 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 organisation. Processing personal data on behalf of another organisation refers to the carrying out of any operation or set of operations in relation to the personal data and includes, but is not limited to, the organisation, adaptation or alternation; retrieval; and transmission of the said personal data.

31 Section 4(2) of the PDPA confers an obligation on the data intermediary to comply with the Protection Obligation and the obligation to cease to retain personal data under ss 24 and 25 of the PDPA respectively.

---

1 Act 26 of 2012.

32 In addition, s 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

Issue (a): What obligations did each of the Respondents owe under the PDPA in respect of the Complainant's personal data?

Smiling Orchid

33 It is not disputed that Smiling Orchid, being an organisation which has its customers' personal data in its possession and/or under its control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, pursuant to s 24 of the PDPA.

34 This is so regardless of whether Smiling Orchid had appointed a data intermediary or data intermediaries to process customer personal data on its behalf. As such, Smiling Orchid is required to comply with s 24 of the PDPA and adopt or ensure the adoption of security arrangements that are reasonable and appropriate in the circumstances.

T2

35 In light of the facts and representations made by Smiling Orchid and T2, the Commission understands that T2 had not been engaged by Smiling Orchid to carry out any processing activities with regard to personal data on its behalf. Therefore, it cannot be said that T2 is a data intermediary processing personal data on behalf of Smiling Orchid.

36 First, as noted at [17] above, the security of the site or the CMS was not part of T2's scope of work under the Project Agreement and Smiling Orchid conceded that T2 was engaged mainly to enhance the design of its website.

37 Second, the Commission notes that T2 did not deal with any personal data of Smiling Orchid's customers. Accordingly, none of the Complainant's personal data can be said to have been in T2's possession or under T2's control at the material time.

38 Hence, even though Smiling Orchid represented that it had depended on T2 to be "in charge of the site" and T2 itself represented that it had investigated the cause of the Data Breach Incident and carried out corrective measures upon being informed of the Data Breach Incident in February 2015 and on other occasions, the Commission is satisfied that there was no evidence that T2 was charged with the responsibility to secure the personal data as a data intermediary.

39 Accordingly, T2 did not have an obligation under s 24 of the PDPA to protect the personal data on Smiling Orchid's website.

Cybersite

40 The Commission considers that Cybersite was a data intermediary of Smiling Orchid for the purposes of the PDPA. Cybersite was the hosting service provider for Smiling Orchid's website at the material time and, as noted at [8] above, it had in its possession the personal data of Smiling Orchid's customers stored on its servers in Singapore.

41 Pursuant to ss 4(2) and 4(3) of the PDPA, Cybersite had an obligation to make reasonable security arrangements to protect the personal data of Smiling Orchid's customers.

East Wind

42 East Wind is a data intermediary of Smiling Orchid for the purposes of the PDPA as it is an IT service provider and processed personal data on behalf of Smiling Orchid.

43 Since East Wind was only appointed by Smiling Orchid after the Data Breach Incident and was not involved in any part of the site during the material time, the Commission is of the view that East Wind's role does not factor into its considerations pertaining to the Data Breach Incident.

Issue (b): Did each of the Respondents comply with their obligation under section 24 of the PDPA in respect of the Data Breach Incident?

Smiling Orchid

44 After carefully considering all the relevant facts and representations made by the Respondents, the Commission is of the view that Smiling Orchid failed to take reasonable security measures to protect the customers' personal data in its possession and/or under its control.

45 First, the Commission found that there was no clear designation of security responsibilities by Smiling Orchid. As noted at [17] and [18] above, Smiling Orchid represented that it had depended on T2 to be "in charge of the site" but T2 denied that it was responsible for Smiling Orchid's website security at the time of the Data Breach Incident.

46 As an organisation subject to the data protection provisions of the PDPA, Smiling Orchid is ultimately responsible for ensuring that there are reasonable security arrangements in place to protect the personal data in its possession and/or under its control; further, that any data intermediary that processes personal data on its behalf complies with the PDPA. In this case, it would appear that prior to the Commission's investigation, Smiling Orchid had not even considered that it was required to implement reasonable security measures to ensure that the personal data in its possession and/or under its control were adequately protected in accordance with s 24 of the PDPA. Smiling Orchid had merely relied on T2 to be "in charge of the site" without properly engaging T2 to provide security oversight for the site. The omission to do so discloses the lack of implementing security arrangements for the site.

47 Second, the investigations undertaken by T2 were poorly conducted and the corrective actions it performed by reinserting the line of code and changing the administrator and server passwords were superficial and did not address the root cause of the incident. Consequently, a breach caused by the same line of code being removed had occurred again in November 2015 and T2 had again performed the same ineffective corrective actions. That the line of code had been removed on more than one occasion showed that Smiling Orchid had failed to ensure that adequate corrective actions were performed to resolve the root cause of any unauthorised access and/or disclosure. It also demonstrated an inadequate understanding of IT security that fell below reasonably expected standards.

48 Third, even though the issue was made known to Smiling Orchid in November 2014, even as late as October 2015, Smiling Orchid had only undertaken corrective actions in one domain even though there were two domains involved. The same security issue had also arisen again in November 2015 even after the whole system was ported to a new hosting environment. Furthermore, since T2 has yet to identify the actual cause of the code removal, Smiling Orchid is unable to say that the corrective actions that T2 had undertaken would be enough to address this problem.

49 In addition, as noted at [26] above, T2 admitted that the protection of accounts and passwords were weak: *ie*, CMS passwords, including the administrator user passwords, were stored in plain text and were unprotected, and there was a lack of a policy relating to password length and strength.

50 New administrator accounts and passwords in relation to the CMS could be created by any existing administrator account holder and there was no indication of any policy or logs as to who maintains these accounts and removes unused accounts. While the absence of a policy for the protection and accountability of the administrator user accounts is not directly related to the cause of the Data Breach Incident, the Commission is of the view that this demonstrates an overall lack of security awareness on the part of Smiling Orchid and a failure to make reasonable security arrangements.

51 It is unclear whether T2's actions would have been different had it been engaged to do more than enhancing the design of the site. Data controllers that engage outsourced service providers have to be clear about the nature and extent of services that the service provider is to provide. There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services. In the absence of such clarity of intent and procedures, it is risky to hold that the outsourced service provider is a data intermediary. In any case, the Commission has found that T2 is not a data intermediary for the reasons set out at [35] to [38] above.

52 Consequently, in view of all the relevant facts and circumstances, the Commission is not satisfied that Smiling Orchid has made reasonable security arrangements to prevent unauthorised access, collection, use,

disclosure, copying, modification, disposal or similar risks in compliance with the Protection Obligation under s 24 of the PDPA.

Cybersite

53 As a data intermediary of Smiling Orchid, Cybersite has an obligation to comply with the Protection Obligation under s 24 of the PDPA.

54 In this case, there was no evidence of Cybersite being in breach of its Protection Obligation under s 24 of the PDPA.

55 For the general security of its servers, Cybersite had put in place security arrangements including regular changing of system passwords, and regular updates of its firewall(s), anti-virus software and anti-spam software. There was no evidence that these security measures had been compromised or of Cybersite's servers being hacked at the material time.

56 Relating to the data breach that had occurred in this case, the security issues that were identified were at the application-level (*ie*, the CMS). It was found that these issues did not pertain to the contracted responsibilities of Cybersite, who was only hosting the site. Although T2 had hypothesised that the code was removed because someone had hacked into the system by gaining access to Cybersite's servers where the code is stored to remove the code, as mentioned above, there was no evidence of cyber-hacking into Cybersite's servers at the material time. In any event, the same issue occurred even after Smiling Orchid had switched hosting service providers.

57 Accordingly, the Commission does not find Cybersite to be in breach of s 24 of the PDPA.

ENFORCEMENT ACTION TAKEN AGAINST SMILING ORCHID

58 Having completed its investigation and assessment of this matter, the Commission finds that Smiling Orchid is in breach of s 24 of the PDPA.

59 In exercise of the power conferred upon the Commission pursuant to s 29 of the PDPA, the Commission directs that a financial penalty of $3,000 be imposed on Smiling Orchid.

60 The Commission also directs that:

(a) Smiling Orchid shall, within 120 days from the date of the Commission's direction:

(i) put in place the security arrangements for the new website to protect the personal data that were collected, or may be collected, by Smiling Orchid;

(ii) conduct a web application vulnerability scan of the new website;

(iii) patch all vulnerabilities identified by such vulnerability scan; and

(b) by no later than 14 days after the above action has been carried out, Smiling Orchid shall, in addition, submit to the Commission a written update providing details on (i) the results of the vulnerability scan; and (ii) the measures that were taken by Smiling Orchid to patch all vulnerabilities identified by the vulnerability scan.

61 The Commission took into account the following factors in assessing the breach and the directions to be imposed:

Smiling Orchid

(a) Smiling Orchid was not forthcoming nor co-operative in providing the full details of what transpired and its IT outsourcing agreements during the Commission's investigation. In fact, despite the issuance of one Notice to Require Production of Documents and Information under the Ninth Schedule to the PDPA to Smiling Orchid and several verbal clarifications over the phone, the Commission was still unable to establish the pertinent facts on what caused the discourse and the specific roles of the parties involved at the material time. As a result, the Commission had to take statements from the relevant parties in order to gather and distil facts;

(b) there was a recurring breach of the exact same nature in November 2015, even after Smiling Orchid had been informed of the Data Breach Incident by the Commission in February 2015. Every time a data breach occurred, the same ineffective corrective action would be taken by putting back the lines of codes protecting the site content by the administrator password without ascertaining the root cause of the repeated breaches;

(c) Smiling Orchid's entire database was potentially at risk of being disclosed if someone possessed the know-how to change the digits in the URL link;

(d) even though Smiling Orchid is a small-medium enterprise without internal IT knowledge and expertise, as an organisation under the PDPA, it is ultimately responsible for protecting the personal data

in its possession and/or under its control pursuant to s 24 of the PDPA;

(e) the impact of the data breach appears to have been limited; and

(f) Smiling Orchid has taken some steps to remedy the breach, including engaging a new IT vendor, East Wind, to revamp Smiling Orchid's website.

T2 and Cybersite

(g) The Commission finds that T2 and Cybersite appeared to play a significant role in this matter. T2 was essentially Smiling Orchid's main IT vendor and Smiling Orchid was heavily dependent on T2 in respect of its entire IT system. However, T2 had a superficial understanding of the IT system. Its repeated outsourcing of different tasks to different parties, who in turn re-outsourced the tasks, also resulted in confusion as to which party was responsible for the defective line of code that eventually led to the Data Breach Incident. Notwithstanding, as T2 was only engaged to provide web designing services and not website security and it did not handle or process personal data at the material time of the Data Breach Incident, the Commission finds that T2 was not a data intermediary of Smiling Orchid and was not in breach of the Protection Obligation under the PDPA.

(h) Cybersite, which was the domain and hosting provider for Smiling Orchid, also has an important role to protect the personal data of Cybersite's customers that were held on its servers. Although the Commission has not found Cybersite to be in breach of the Protection Obligation under s 24 of the PDPA, the Commission is of the view that a timely reminder should be issued to the organisation on its obligation as a domain and hosting provider in view of the data breach that had taken place.

(i) The Commission will be issuing advisory notices to T2 and Cybersite on their roles and obligations mentioned above.

East Wind

(j) The Commission notes that East Wind was Smiling Orchid's newly-appointed IT vendor that provided assistance and support in terms of security know-how during the investigation and was not involved in any way at the material time.

62 The Commission emphasises that it takes a very serious view of any instance of non-compliance under 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.

YEONG ZEE KIN
Deputy Commissioner
Personal Data Protection Commission

Grounds of Decision

Re My Digital Lock Pte Ltd

Case Number: DP-1601-A628
Decision Citation: [2016] SGPDPC 20

Consent Obligation *– Disclosure of personal data without consent*
Consent Obligation *– Disclosure of personal data without consent – Investigations or proceedings exception*
Consent Obligation *– Disclosure of personal data without consent – Provision of legal services exception*
Consent Obligation *– Disclosure of personal data without consent – Publicly available exception*
Liability of employers for acts of employees *– Whether employee was acting in the course of employment*
Protection Obligation *– Insufficient technical and administrative security arrangement*

4 November 2016

BACKGROUND

1 On 4 January 2016, the Complainant complained to the Personal Data Protection Commission ("Commission") that the Respondent had disclosed his personal data by posting screenshots of the Complainant's WhatsApp conversations with the Respondent's director, [redacted] ("Mr A"), on Mr A's Facebook page.

2 On account of the complaint made, the Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether the Respondent had breached its obligations under the PDPA. The material facts of the case are as follows.

1 Act 26 of 2012.

MATERIAL FACTS AND DOCUMENTS

3 The Respondent is in the business of selling digital locks and doors. The Complainant had made a purchase of a gate from the Respondent for his home.

4 Subsequently, the Complainant and the Respondent became involved in a dispute concerning alleged defects in the gate. The parties were engaged in legal proceedings in relation to certain remarks that were allegedly made by the Complainant concerning the Respondent's product, business and/or service. On 4 January 2016, Mr A posted screenshots on his Facebook page of his previous WhatsApp messages (including photographs) that were exchanged between the Complainant and Mr A in connection with the dispute. In posting the screenshots on Facebook, the screenshots were made publicly viewable. The screenshots contained the Complainant's personal mobile phone number and his residential address ("Complainant's Personal Data"). The Complainant became aware of this and lodged his complaint.

5 On 1 March 2016, the Commission notified the Respondent of the complaint and sought assistance in investigations. In the course of the investigations, the Respondent accepted that there was a public disclosure of the Complainant's Personal Data on Mr A's Facebook page but represented to the Commission that:

(a) Mr A had posted the screenshots containing the Complainant's Personal Data on Mr A's Facebook page for the purposes of transferring the screenshots from Mr A's WhatsApp application to Mr A's desktop computer;

(b) the transfer was to enable Mr A to send the screenshots to the Respondent's solicitors in connection with the court proceedings between the Respondent and the Complainant;

(c) Mr A removed the screenshots containing the Complainant's Personal Data from his Facebook page about an hour after they were posted, after Mr A had transferred the screenshots to his desktop computer;

(d) the Complainant's Personal Data was disclosed by Mr A in his personal or domestic capacity;

(e) the Complainant's Personal Data disclosed was publicly available data; and

(f) the Complainant's Personal Data was disclosed pursuant to investigations and proceedings, in particular the civil proceedings

between the Complainant and the Respondent that were contemplated then and which have since been commenced.

6 In support of the Respondent's claim that the Complainant's Personal Data was publicly available information, the Respondent provided a screenshot of a YouTube video and five images from online sites which purport to show that the personal data of the Complainant was previously available online. According to the Respondent, the YouTube video is no longer accessible online.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Issues to be determined

7 The Respondent admits to the posting of the screenshots on Facebook by Mr A. As the posting of the screenshots was a deliberate act by Mr A, and it caused the screenshots to be published on Facebook, this amounted to a disclosure made by Mr A of the Complainant's Personal Data.

8 Even though Mr A claims that he did not intend to disclose the Complainant's Personal Data to third parties, the fact is that he had made the disclosure on a social media and networking application, which has the function of broadcasting and sharing text messages, pictures, *etc*, to the Facebook community. The size of the Facebook community and thus the extent of disclosure depends on the privacy policy settings on Mr A's Facebook page. On the evidence, this was set to allow friends of Mr A to view the page. Mr A's intentional act of uploading the screenshots on a medium used for broadcasting or sharing of media was therefore, in the Commission's view, an act of disclosure of the Complainant's Personal Data. This is not a case where the Respondent had uploaded the screenshots to a secured online file storage or repository platform that limits access to his solicitors, which may have supported his defence that the disclosure was pursuant to an exception in the Fourth Schedule to the PDPA.

9 The issues arising from the case are as follow:

(a) whether the disclosure of the Complainant's Personal Data on Facebook without the Complainant's prior consent was permitted under ss 13 and 17 of the PDPA ("Issue A");[2] and

(b) whether the Respondent had breached s 24 of the PDPA[3] in relation to its use of Mr A's Facebook page as a means of transferring the Complainant's Personal Data ("Issue B").

10 It should also be noted that even though this was a case of a disclosure of the Complainant's Personal Data, the Protection Obligation under s 24 of the PDPA is also relevant in this case, given the lackadaisical manner in which the Complainant had sought to transfer the screenshots to his lawyers. The Protection Obligation is a separate obligation which an organisation would need to comply with on top of the other obligations under the PDPA. In a case where the security of the personal data features as an issue, the Commissioner will investigate into the Protection Obligation as well.

11 Based on the two issues mentioned above, the Commission's assessment on these issues are set out below.

Issue A: Whether the Respondent has complied with its Consent Obligation in disclosing the Complainant's Personal Data on Facebook

Sub-issue I: Whether the Respondent is responsible for Mr A's disclosure of the Complainant's Personal Data

12 A preliminary question is whether the Respondent is responsible for Mr A's disclosure of the Complainant's Personal Data. Under s 53(1) of the

---

2 In essence, under ss 13 and 17 of the Personal Data Protection Act 2012 (Act 26 of 2012), an organisation is prohibited from disclosing personal data about an individual without consent, or deemed consent, unless an exception applies pursuant to s 17.

3 Section 24 of the Personal Data Protection Act 2012 (Act 26 of 2012) requires an organisation to protect personal data in its possession or under its control by taking reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

PDPA, any acts done or conduct engaged in by an *employee in the course of his employment* shall be treated for the purposes of the PDPA as done or engaged in by his employer as well as him, whether or not it was done or engaged in with the employer's knowledge or approval.

13 Based on the facts described at [3] to [5] above, the Commission is satisfied that Mr A was acting in the course of his employment as a director of the Respondent when transferring the Complainant's Personal Data through his Facebook page. The Commission disagrees with the Respondent's claim that Mr A was transferring the Complainant's Personal Data in his personal or domestic capacity. This is because the Respondent asserts that the transfer was for the purposes of sending screenshots containing the Complainant's Personal Data to the Respondent's solicitors, which was in connection with the dispute between the Respondent and the Complainant. The Commission notes that civil proceedings have since been commenced by the Respondent against the Complainant.

14 Accordingly, Mr A's disclosure of the Complainant's Personal Data is treated as a disclosure by the Respondent since it was made in the course of employment pursuant to s 53(1) of the PDPA.

Sub-issue: II: Given that the disclosure was made without the Complainant's consent, whether the Complainant's Personal Data was publicly available data and disclosure necessary for investigations and proceedings

15 It is not disputed that the Respondent did not have the consent of the Complainant when disclosing the Complainant's Personal Data on Facebook. However, the Respondent claims that the Complainant's Personal Data was, firstly, publicly available data and, secondly, that the disclosure was necessary for investigations and proceedings by the Respondent. If either exceptions are met, the Respondent would be permitted to disclose the Complainant's Personal Data without having to obtain the Complainant's consent.

16 Upon an examination of the facts disclosed during investigations, the Commission finds that these two exceptions do not apply to this case for the following reasons below.

Publicly available data

17 Pursuant to s 17 of the PDPA and para 1(*d*) of the Fourth Schedule to the PDPA, an organisation may disclose personal data of individuals without consent, if the personal data is publicly available. As mentioned at [6] above, the Respondent had produced a screenshot and images of online sites to the Commission to show that the Complainant's information was previously available to the public online.

18 Having perused these documents, the Commission finds that none of these documents contain the Complainant's Personal Data. While these documents may contain some other information, such as the front entrance of the Complainant's apartment, or portions of the *content* from WhatsApp conversations between the Complainant and the Respondent, these are not relevant to the assessment of whether the Complainant's Personal Data was also publicly available information.

19 Since there was no further evidence that was proffered to show that the Complainant's Personal Data was publicly available information, the Commission finds that the Respondent may not rely on s 17 and para 1(*d*) of the Fourth Schedule to the PDPA for disclosing the Complainant's Personal Data without consent.

Disclosure necessary for investigations and proceedings by the Respondent

20 The Respondent sought also to rely on the exceptions in paras 1(*f*) and 1(*j*) of the Fourth Schedule to the PDPA, read with s 17 of the PDPA. In essence, these exceptions allow for disclosure of personal data to be made without consent where the disclosure was (a) necessary for any investigation or proceedings; or (b) necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services.

21 In both these exceptions, there is a requirement to show that the disclosure to be made was "necessary" for the purposes set out in paras 1(*f*) and 1(*j*) of the Fourth Schedule. Based on the facts of this case, the Respondent has failed to show that he needed to make the disclosure (a) on Facebook; and/or (b) to Mr A's contacts on Facebook, for the purposes set out in paras 1(*f*) and 1(*j*) of the Fourth Schedule. All that appears to be needed, and all that he claims he intended to do, was to transfer the files to

his lawyers, which did not require him disclosing the Complainant's Personal Data to other third parties. As the Respondent itself admits, there were other ways by which Mr A could have sent the screenshots to his solicitors.

22 In the premises, the Commission finds that the exceptions under paras 1(*f*) and 1(*j*) of the Fourth Schedule to the PDPA do not apply to the case.

23 Given that the disclosure was made without the consent of the Complainant, and that none of the exceptions raised by the Respondent above would apply, the Respondent is in breach of s 13 of the PDPA.

Issue B: Whether the Respondent had complied with section 24

24 The Complainant's Personal Data transferred by the Respondent included the Complainant's mobile number and residential address. There is no doubt that these data fall within the definition of "personal data" under the PDPA since the Complainant may be identified from such data when the data are coupled with other information which the Respondent has. There is also no dispute that at the material time, the Complainant's Personal Data was within the possession or control of the Respondent.

25 In the Commission's view, the manner and mode by which the Complainant's Personal Data was transferred over Facebook was wholly inappropriate. Even if the period of the transfer is short, there exists a substantial risk of the Complainant's Personal Data being viewed, observed or even collected by persons, with no necessity to do so. Reasonable or adequate security arrangements when transferring personal data must at least involve a process where the personal data are reasonably protected from unauthorised access or interference, until the personal data reaches their intended destination or recipient where other security arrangements on storage would apply. For example, the file could have been encrypted (or at least password protected) so that only authorised people can access its content. Alternatively, the photographs could at least have been uploaded to a site which permits control of access to the files, instead of making it visible to a wider audience on *an open social media platform* such as Facebook which dramatically increases the risk of unauthorised access or collection, and subsequent misuse. Lastly, it is not clear why a transfer over the open Internet was preferable, as Mr A could have simply connected his phone to

his PC and transferred the file without the need to make use of the open Internet.

26 In view of the above, the Commission finds that the Respondent had failed to make reasonable security arrangements to protect personal data in its possession or under its control when transferring the Complainant's Personal Data using Mr A's Facebook page. As such, the Respondent is in breach of s 24 of the PDPA.

ACTIONS TAKEN BY THE COMMISSION

27 Given the Commission's findings that the Respondent is in breach of its obligations under ss 13 and 24 of the PDPA, the Commission is empowered under s 29 of the PDPA to issue the Respondent 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 $1m.

28 In determining the direction, if any, to be made, the Commission considered the following factors:

(a) the Complainant's Personal Data was only exposed on Mr A's Facebook page for a short period of time of about an hour;

(b) the breach involved personal data of limited sensitivity (*ie*, the Complainant's mobile number and residential address);

(c) the breach was not wilful or due to systemic failures of the Respondent's policies or processes but was instead triggered by an error of judgment of a single employee, *ie*, Mr A; and

(d) the Respondent had been fully co-operative in the investigation.

29 In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning to the Respondent for the breach of its obligations under ss 13 and 24 of the PDPA.

YEONG ZEE KIN
Deputy Commissioner
Personal Data Protection Commission

Grounds of Decision

Re Jump Rope (Singapore)

Case Number: DP-1411-A265
Decision Citation: [2016] SGPDPC 21

Consent Obligation *– Disclosure of personal data without consent – Reasonableness of disclosure*
Notification Obligation *– Disclosure for the purpose of managing or terminating an employment relationship*
Notification Obligation *– Disclosure of personal data without notification*
Purpose Limitation Obligation *– Disclosure of personal data for purposes that a reasonable person would consider appropriate in the circumstances*

24 November 2016

BACKGROUND

1 On 1 December 2014, the Personal Data Protection Commission ("Commission") received a complaint against Jump Rope (Singapore) ("Respondent") from a complainant ("Complainant") alleging that his personal data had been disclosed in an e-mail sent to various Singapore government schools.

2 The Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether there had been a breach by the Respondent of its obligations under the PDPA.

MATERIAL FACTS AND DOCUMENTS

3 The Respondent is a non-profit society registered with the Registry of Societies that promotes and manages the sport of rope skipping, and provides training to students in Singapore schools. The Respondent was set up by the President of the Respondent, [redacted], who is also the owner

1 Act 26 of 2012.

and director of Emotion Learning Pte Ltd ("Emotion") and Eltitude Pte Ltd ("Eltitude"). Emotion and Eltitude are companies in the business of providing enrichment and CCA education, and enrichment and sports coaching services to schools respectively.

4 Based on the Respondent's response to the Commission during the investigation, the Commission understands that the Complainant was a former employee of Emotion and Eltitude, who held the designation of Part Time Instructor. The Complainant went through an in-house training programme conducted by Emotion, and obtained a certificate in rope skipping coaching, which was issued by the Respondent.

5 The Respondent alleged that the Complainant had breached his contract of employment with his employers and had engaged in some unethical activities during the course of his employment. As a result, the Respondent blacklisted the Complainant and revoked his certification.

6 The President of the Respondent then decided to send an e-mail to various government schools involved in the sport of jump rope to notify them of the blacklisting of the Complainant and the revocation of his certification. In this regard, an e-mail dated 28 November 2014 originating from the e-mail address admin@jumpropesingapore.com was sent to around 30 government schools ("E-mail"). The E-mail stated, among other things, that disciplinary action had been taken against the Complainant, and that he was on the Respondent's blacklist. The E-mail set out the Complainant's name and NRIC number (and the name and NRIC number of another individual), and stated that persons on the blacklist are not suitable for instructing and coaching duties in schools. The Respondent advised all schools not to engage the named persons to avoid the teaching of wrong values to their pupils.

7 In addition, the Respondent stated that as a non-profit rope skipping society with the mission to monitor and protect the interest of the sport and the children, the Respondent considered it necessary to inform the schools involved in rope skipping, so that the schools could take precautions. The E-mail was sent to around 30 government schools involved in rope skipping, and it was solely meant to inform the schools of the situation. The Respondent's stated intentions in sending the E-mail was to provide schools with information which may be important in their decision when engaging rope skipping instructors, so that the schools can better decide in engaging the appropriate people to teach, instruct and coach their students. The

Respondent reiterated that the disclosure of the personal data of the Complainant was meant solely to help schools in decision making when engaging rope skipping instructors.

8 Having carefully considered the relevant facts and circumstances, including the statements and representations made by the Respondent, the Commission has completed its investigation into the matter, and sets out its findings and assessment herein.

COMMISSION'S FINDINGS AND ASSESSMENT

9 The nub of the Respondent's claim is that it had good intentions when it informed the various government schools involved in the sport of jump rope of the blacklisting of the Complainant and the revocation of his certification. In particular, the following points were noted:

(a) the Respondent claimed that it had advised all schools not to engage the named persons so as to avoid the teaching of wrong values to their pupils; and

(b) the Respondent claimed that it had decided to send out the E-mail to the various government schools to notify them of the blacklisting of the Complainant and the revocation of his certification so that the schools "can better decide on engaging the right people to teach, instruct and coach [their students]", and to take precautions against engaging the wrong rope skipping instructors.

10 It is clear that consent for disclosure of the Complainant's personal data in an e-mail communicating that he had been blacklisted was not obtained. This is not a case where consent was obtained earlier in time when he was first employed; and there is no evidence to show that the Complainant was notified nor gave consent for disclosure, before or after the Complainant had been disciplined and dismissed. In a suitable case, there can be valid business or legal reasons for the blacklisting to be disclosed in order to warn the Respondent's clients, notwithstanding that it may contain some personal data about the Complainant. It may not be desirable to expect organisations to obtain consent from the person(s) that is the subject of the disciplinary action, dismissal and blacklisting, as consent is unlikely to be forthcoming in all cases. However, the organisation should still comply with the neighbouring obligations of consent, namely, the notification obligation and the purpose limitation

obligation. This means disclosing the blacklist containing the former employee's personal data only for purposes that a reasonable person would consider appropriate in the circumstances, and notifying the former employee about the disclosure to be made.

11 In a suitable case, disclosure of personal data that are relevant to the matter, by an organisation without consent nor notification, may be made if it is reasonable to do so. This is because the standard of "reasonableness" underpins the PDPA, as specifically provided for under s 11(1) of the PDPA. Section 11(1) of the PDPA provides that "[i]n meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances". In this regard, an organisation can inform its clients that Person A (name and former designation) has left its employment on a specific date. Further, the Commission considers that it is conceivable that there can be circumstances where an organisation may be acting reasonably in disclosing personal data in respect of a blacklisting to warn others, without consent, and apart from the scheduled exceptions; but these are limited, and very much depends on the context and circumstances in which the disclosure was made. For example, if there was credible evidence of fraudulent conduct that a former member of staff is misrepresenting his status of employment and association with his former employer, it may be reasonable for the former employer to write to existing customers informing them of the facts. The former employer should, however, also inform the former member of staff of the communication to be made to the existing customers, so that the disclosure of personal data is made transparent to the member of staff concerned.

12 In this case, not only has the Respondent failed to obtain consent from the Complainant for the disclosure made pursuant to ss 13 to 15 of the PDPA, the Respondent's actions have gone beyond what is reasonable in the circumstances. The Commission has not found any business or legal reasons that justifies the Respondent's actions in writing to its clients to inform them of the blacklisting. It is not uncommon for employees to leave for various reasons, including for poor performance and breaches of codes of conduct. In the absence of evidence that the Complainant's post-employment conduct had put the Respondent's trade reputation or potential clients at risk, the Respondent's measure of writing to name and shame the Complainant is not an appropriate or reasonable step to take.

13 Given the potential adverse effect or consequence on the Complainant from the disclosure of such information to third parties, in particular, the impact on future engagements of the Complainant's services for jump rope activities, the Respondent ought to have taken the extra care and precautions in relation to the protection and disclosure of personal data of the Complainant. But based on the assessment above, it did not appear to the Commission that the Respondent had afforded the appropriate care, protection and sensitivity to the data that it was disclosing. The Respondent's actions in the circumstances were unreasonable.

14 For completeness, the Commission considered whether s 20(4) of the PDPA, which provides that an organisation must inform the individual of the purpose of disclosure where the collection, use or disclosure was made for the purpose of managing or terminating the employment relationship between the organisation and the individual, is applicable in the present case. In the Commission's view, s 20(4) of the PDPA is not relevant as it deals with collection, use or disclosure for the purpose of either managing an ongoing employment relationship or for the purpose of terminating an employment relationship. In the present case, the employment relationship between the Complainant and the Respondent had already been terminated by the time the disclosure through the E-mail took place.

15 On account of the above, the Respondent is in breach of ss 11, 13 and 20 of the PDPA.

ENFORCEMENT ACTION BY THE COMMISSION

16 Given the Commission's findings that the Respondent is in breach of ss 11, 13 and 20 of the PDPA, the Commission is empowered under s 29 of the PDPA to give the Respondent 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 $1m as the Commission thinks fit.

17 In considering whether a direction should be given to the Respondent in this case, the Commission considered the following:

(a) the disclosures were made to a limited number of government schools;

(b) the personal data that were disclosed were limited, and were in relation to limited individuals; and

(c) the Respondent had been co-operative with the Commission and forthcoming in its responses to the Commission during the Commission's investigation.

18 In view of the factors set out above, and having regard to the overall circumstances of the matter, the Commission has decided not to issue any direction to the Respondent to take remedial action or to pay a financial penalty. Instead, the Commission has decided to issue a Warning to the Respondent for breach of its obligations under ss 11, 13 and 20 of the PDPA.

YEONG ZEE KIN
Deputy Commissioner
Personal Data Protection Commission

Grounds of Decision

Re The Cellar Door Pte Ltd and another

Case Number: DP-1409-A099
Decision Citation: [2016] SGPDPC 22

Data intermediary *– Obligations of organisation and data intermediary*
Data intermediary *– "Processing" of personal data*
Protection Obligation *– Disclosure of personal data – Insufficient technical and administrative security arrangements*

23 December 2016

BACKGROUND

1 On or around September 2014, the Personal Data Protection Commission ("Commission") found unauthorised postings on a website (<http://pastebin.com/jiQw38nU>) known as "Pastebin", comprising personal data of customers of The Cellar Door Pte Ltd ("Cellar Door") and users of Cellar Door's website (collectively, the "customers"), which was made available online.

2 The Commission undertook an investigation into the matter and its findings and grounds of decision are set out below.

MATERIAL FACTS AND DOCUMENTS

3 Cellar Door is in the business of selling food and wine products, and has a business website with the address <http://www.thecellardoor.com.sg> (the "Site").

4 The Site was developed by a company known as Global Interactive Works Pte Ltd ("GIW"), which specialises, amongst other things, in website design, development and hosting. GIW was engaged to design and develop the Site. The Site and Cellar Door's customer database were hosted on GIW's server. As part of these services, GIW would also backup the Site and customer database. Only GIW's staff would have access to these backups.

5 The disclosure of personal data on Pastebin was comprised of the full names, mobile and residential telephone numbers, residential addresses, e-mail addresses and passwords of Cellar Door's customers. The data that was disclosed on the Pastebin website was a subset of Cellar Door's entire customer database. Cellar Door was not aware of the unauthorised disclosure on the Pastebin website prior to the Commission informing Cellar Door of the said disclosure.

6 In response to the Commission's inquiry into the matter, GIW stated that its engineers were unable to determine the reasons for the disclosure of the personal data of Cellar Door's customers on the Pastebin website. GIW developed the Site for Cellar Door in 2011. Subsequent to that, Cellar Door engaged GIW to host the Site and Cellar Door's customer database, but it did not sign up for a maintenance package to maintain its Site and customer database.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Issues for determination

7 The issues to be determined in the present case are as follows:

(a) Whether GIW was acting as a data intermediary for Cellar Door in relation to the personal data hosted on GIW's servers.

(b) If GIW is a data intermediary for Cellar Door, what were the respective obligations of GIW and Cellar Door under the Personal Data Protection Act 2012[1] ("PDPA").

(c) Whether Cellar Door and GIW had complied with their obligations under s 24 of the PDPA.

Relevant provisions

8 Section 24 of the PDPA provides that an organisation is obliged to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use,

1 Act 26 of 2012.

disclosure, copying, modification, disposal or similar risks ("Protection Obligation").

9 Section 4(2) of the PDPA confers an obligation on the data intermediary to comply with the Protection Obligation and the obligation to cease to retain personal data under ss 24 and 25 of the PDPA respectively.

10 Further, s 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

Issue A: Whether GIW is a data intermediary for Cellar Door

11 GIW was engaged by Cellar Door to host the Site and customer database on its servers. The set of operations that GIW would carry out in furtherance of this engagement, such as the storage or holding of personal data on GIW's servers, or the organisation or management of personal data in the customer databases, would fall squarely within the definition of "processing" under s 2(1) of the PDPA. As such, GIW was processing the personal data of Cellar Door's customers.

12 As GIW carried out the abovementioned operations on behalf of Cellar Door and for its business purposes, GIW comes under the definition of a "data intermediary" under the PDPA, and is therefore required to comply with the Protection Obligation.

Issue B: Cellar Door's and GIW's respective obligations under the PDPA

13 Having determined that GIW is a data intermediary for Cellar Door, it is appropriate for the Commission to elaborate on the respective obligations of Cellar Door and its data intermediary, GIW, under s 24 of the PDPA in respect of the personal data in question.

14 Pursuant to ss 4(2) and 4(3) of the PDPA, both Cellar Door and GIW are obliged under s 24 of the PDPA to ensure that there are reasonable security arrangements to protect the personal data of Cellar Door's customers.

15 In the Commission's view, Cellar Door has the primary responsibility of ensuring the overall protection of the personal data, and it was for

Cellar Door to put in place the necessary security measures to protect the personal data. Cellar Door is not discharged of its responsibility simply because it had engaged a data intermediary (*ie*, GIW) to provide hosting and database services for Cellar Door. It is incumbent on Cellar Door to take the necessary steps to ensure the overall protection of data, even though it may have engaged GIW to assist with certain data operations. For example, Cellar Door may put in place contractual arrangements which clearly define the scope of GIW's responsibilities, and follow through with operational procedures and checks to ensure that GIW carries out its functions.

16 GIW, on the other hand, has the direct responsibility of ensuring the protection of the personal data, as it was hosting the personal data on its servers, and was the site administrator for the Site and customer database. GIW would therefore also need to ensure that reasonable security arrangements are put in place to protect the personal data in its possession or under its control. The extent of GIW's obligations are scoped in accordance with the contractual arrangement it had with Cellar Door. In this case, it is the protection of the customer database hosted by it.

17 A secondary issue in this case would be the distinction between possession and control of personal data. The Commission is of the view that it is possible for the same data set of personal data to be in the possession of one organisation, and under the control of another. For example, in a situation where the organisation transfers personal data to its data intermediary, the organisation could remain in control of the personal data set while, simultaneously, the data intermediary may have possession of the same personal data set.

18 In the present case, the Commission finds that the personal data handled by GIW were still under the control of Cellar Door, given that GIW was Cellar Door's service provider, and the personal data that GIW had processed (as defined in the PDPA, and examined at [11] and [12] above), were for Cellar Door's business purposes.

19 Accordingly, even though Cellar Door was not in direct possession of the personal data that were held in GIW's servers, it was still obliged to protect the data by operation of s 4(2) of the PDPA (as mentioned at [14] above), and, additionally, by the fact that it had control over the personal data (as found at [18] above).

20 The Commission now turns to its assessment of whether Cellar Door and GIW have complied with their obligations under s 24 of the PDPA respectively.

Issue C: Whether Cellar Door and GIW have complied with their obligations under section 24 of the PDPA

21 From its investigations, the Commission has found that there was a lack of adequate security arrangements in place to protect the personal data in question pursuant to s 24 of the PDPA. Broadly, it was found that Cellar Door and GIW had (a) inadequate security policies and processes to protect the personal data; and (b) failed to put in place an overall security to guard against intrusions, attacks or unauthorised access.

Inadequate security policies and processes

22 Having in place adequate security policies and processes is the cornerstone for protecting personal data in the information technology ("IT") setting. In the Commission's view, an adequate security policy should be based on the organisation's assessment of the risks, vulnerabilities and threats facing the IT system and its determination of what the system needs to address these risks, vulnerabilities and threats. In turn, the processes of the organisation can be built upon the security policy that the organisation had put in place. This ensures oversight, proper accountability of the personal data, and control over the measures and processes protecting the personal data.

23 Without such a security policy in place, an organisation may not, amongst other things, be able to detect that a data breach has happened, may not be able to determine what went wrong, and may not know what the corrective measures to be taken are. This was what has happened in this case.

24 In the Commission's view, the organisation, and not the data intermediary, has the primary responsibility of putting in place adequate security policies and processes. In this case, the Commission found several key issues in the system's policies and processes

25 First, Cellar Door had not carried out and had no plan to carry out (prior to the data breach that has happened) penetration testing on the IT system, which meant that there was no systematic way of identifying

vulnerabilities. Further to what was mentioned above at [22], this posed a limitation to Cellar Door's ability to determine the technical measures that are required to ensure that the personal data held by GIW is adequately protected.

26 Second, Cellar Door did not have an ongoing maintenance process to maintain the website and to regularly update or patch it against the latest risks and vulnerabilities. GIW had informed the Commission that Cellar Door did not sign a maintenance contract with GIW for the maintenance and "upkeeping [*sic*] of the website and scripts". This was unacceptable as it left the system exposed to new vulnerabilities that regular security patching could have addressed.

27 Third, there was no incident-management policy or process that tracked identification of the technical issues through to their resolution. GIW had essentially left it to its "offshore programmers" to assess how the breach had happened, which came back inconclusive.

28 In the Commission's assessment, given these shortcomings in the policies and processes above, the Respondents, in particular, Cellar Door, did not provide the necessary oversight, accountability and control for the proper protection of the personal data of Cellar Door's customers.

Failure to protect the system against intrusions or attacks

29 Another important aspect of a "reasonable security arrangement" for IT systems is that it must be sufficiently robust and comprehensive to guard against a possible intrusion or attack. For example, it is not enough for an IT system to have strong firewalls if there is a weak administrative password which an intruder can "guess" to enter the system. The nature of such systems requires there to be sufficient coverage and an adequate level of protection of the security measures that are put in place, since a single point of entry is all an intruder needs to gain access to the personal data held on a system. In other words, an organisation needs to have "all-round" security for its system. This is not to say that the security measures or the coverage need to be "perfect", but only requires that such arrangements be "reasonable" in the circumstances.

30 In this case, the Respondents have failed to put such all-round security in place. The Commission has found several significant gaps in the security measures implemented as follow:

(a) **No server firewall installed**. While there was an alleged "software firewall configuration", there was no firewall installed to protect GIW's server itself at the material time. A firewall is fundamental to the security of the server to protect against an array of external cyber threats, and GIW has the responsibility of ensuring that such a fundamental measure is in place for its server. In this case, a dedicated firewall (beyond the alleged software firewall configuration) protecting the server itself was only installed after the data breach incident had taken place.

(b) **Unused ports were not closed**. The unused ports on the server were not closed at the time of the data breach. Leaving unused ports on a server open increases the risk of an external hacker exploiting the services running on these ports. According to Cellar Door, GIW has since then blocked all unnecessary ports on the server.

(c) **Login credentials were transferred in clear and unencrypted text**. With regard to the Site's functionality, the Commission found that login credentials (*ie*, user logins and passwords) were being transferred in clear and unencrypted text, indicative of a poor level of security in the system design and implementation. This security vulnerability exposed the hosting environment to potential compromise should the credentials be intercepted. Cellar Door, as the organisation having the overall responsibility and control over the design and functionalities of the Site, has the obligation to ensure that, as part of the design and functionalities of the Site, provisions were made for the security of the transmission of the login credentials. In its original design, the Site did not have such a security feature to protect the transmission of the login credentials – but this was prior to s 24 of the PDPA coming into force on 2 July 2014. However, subsequently when the PDPA came into full effect on 2 July 2014, Cellar Door had the obligation to review the design and functionalities of the Site, and put in place the necessary security arrangements to comply with s 24 of the PDPA. Yet, Cellar Door had failed to do so, and the Site still lacked the necessary measures to secure the transmission of the login credentials.

(d) **Weak administration password**. Another of the corrective actions that the Respondents undertook was to increase the "DB Admin Password", which was only six-characters at the material time. In general, a six-character password is not a strong password. Given that the password was for the admininistration account of a

database with remote access capability, the Respondents' password policy should minimally have required a password with a longer length and a mix of alphanumeric and special characters. The need to have a strong password is fundamental to the security of the database system. Weak passwords increase the chances of an intruder cracking the password and gaining full access to the database system, and, more importantly, the personal data stored therein.

31 The security gaps and issues mentioned above exposed the system to all sorts of risks and attacks, such as penetration attacks, cracking, hijacking, and so on and so forth. Ultimately, an intruder that was able to enter through the gaps in the system and gain access to the system would have gained unauthorised access to the personal data held on that system. In the Commission's assessment, therefore, the lack of all-round security in this case was a breach of s 24 of the PDPA.

Whether GIW is in breach of section 24

32 GIW had the direct responsibility of ensuring the protection of the personal data that were in its possession on its servers pursuant to s 24 of the PDPA. Yet, as set out at [29] and [30] above, there were a number of issues pointing towards the lack of protection of the personal data on GIW's servers. In particular, GIW did not put in place adequate security measures when it failed to install a server-side firewall, close unused ports, and implement stronger administration passwords. Accordingly, GIW is in breach of its obligation under s 24 of the PDPA.

Whether Cellar Door is in breach of section 24

33 Given that GIW is a data intermediary of Cellar Door, it follows from s 4(3) of the PDPA, as mentioned above, that Cellar Door is obliged to protect the personal data processed by GIW as if Cellar Door had processed the personal data itself. As such, the Commission's findings regarding the failure by GIW to fulfil its responsibilities and obligations under the PDPA are equally relevant in determining whether there was a breach of the Protection Obligation by Cellar Door. In particular, as mentioned above at [30(c)], it was Cellar Door that had the overall responsibility and control over the requirement of the Site, and it needed to ensure that necessary

security measures were in-built in the requirement of the Site, at least since the PDPA came into force.

34 Additionally, Cellar Door had the primary responsibility of ensuring the overall protection of the data under s 24 of the PDPA, and to implement the overall measures to protect the data. However, as examined at [22] to [28] above, Cellar Door failed to implement adequate policies or processes to protect the personal data under its control. Instead, based on the evidence produced in the matter, it was apparent to the Commission that Cellar Door had mainly relied on its data intermediary, GIW, to run its IT and data management system.

35 Accordingly, the Commission finds that Cellar Door had similarly breached its obligations under s 24 of the PDPA.

COMMISSION'S DIRECTIONS

36 In assessing the breach and the remedial directions to be imposed, the Commission took into consideration various factors relating to the case, including the mitigating and aggravating factors set out below.

(a) the security measures on the Site to protect the personal data fell below the standard reasonably expected, as highlighted at [22] to [31] above, Cellar Door and GIW had inadequate security policies and processes; they failed to protect the system against penetration attacks; and they had a poor administrator password policy;

(b) Cellar Door and GIW had shown a lack of awareness or knowledge of required security measures expected over the personal data in the Site/their hosting environment. As highlighted at [6], [24], [31] to [34] above, Cellar Door and GIW were unable to show how the personal data had been taken from the Site or hosting environment, and had not shown to the satisfaction of the Commission that there were sufficient safeguards to prevent this from happening;

(c) Cellar Door and GIW had been neither co-operative nor forthcoming in their responses to the Notices to Require Production of Documents and Information under the Ninth Schedule to the PDPA ("NTPs") issued by the Commission as part of its investigation. In this regard, the Commission notes that Cellar Door

and GIW displayed a cavalier attitude by providing incomplete responses to the NTPs issued by the Commission; and

(d) although not all the personal data of the customers of Cellar Door had been disclosed on the Pastebin website, given the inadequacies of the Respondents' security measures, the entire customer database was put at risk.

37 Pursuant to s 29(2) of the PDPA, and having completed its investigation and assessment of this matter, the Commission is satisfied that Cellar Door has breached the Protection Obligation under s 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commission hereby directs Cellar Door to do the following:

(a) Cellar Door shall within 60 days from the date of the Commission's direction:

(i) conduct a vulnerability scan of the Site;

(ii) patch all vulnerabilities identified by such scan;

(b) Cellar Door shall, in addition, submit to the Commission by no later than 14 days after the conduct of the abovementioned vulnerability scan, a written update providing details on:

(i) the results of the vulnerability scan;

(ii) the measures that were taken by Cellar Door to patch all vulnerabilities identified by the vulnerability scan; and

(c) Cellar Door shall pay a financial penalty of $5,000 within 30 days from the date of the Commission's direction, failing which interest, at the rate specified in the Rules of Court[2] in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

38 Pursuant to s 29(2) of the PDPA, and having completed its investigations and assessment of this matter, the Commission is satisfied that GIW has breached the Protection Obligation under s 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commission hereby directs GIW to:

Pay a financial penalty of $3,000 within 30 days from the date of the Commission's direction, failing which interest, at the rate specified in

2 Cap 322, R 5, 2014 Rev Ed.

the Rules of Court in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

39 In this case, the Commission has awarded a higher penalty amount against Cellar Door as, in the Commission's view, Cellar Door retained the primary responsibility and obligation to protect the personal data of its customers as the data controller, as elaborated at [15] above.

40 The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA, and it urges parties to take the necessary action to ensure that they comply with their obligations under the PDPA.

YEONG ZEE KIN
Deputy Commissioner
Personal Data Protection Commission

Grounds of Decision

Re Propnex Realty Pte Ltd

Case Number: DP-1512-A613
Decision Citation: [2017] SGPDPC 1

Exceptions to the Consent Obligation *– Disclosure necessary for any purpose which is clearly in the interest of the individual if consent cannot be obtained in a timely way*
Exceptions to the Consent Obligation *– Disclosure necessary for evaluative purposes*
Protection Obligation *– Disclosure of personal data – Insufficient technical security arrangements*

25 January 2017

BACKGROUND

1 On 28 December 2015, the Personal Data Protection Commission ("Commission") received a complaint from the Complainant in relation to the publication online of the Organisation's internal Do Not Call list containing the personal data of 1,765 individuals, including the Complainant and her sisters ("PropNex DNC List"). Following the Complainant's complaint, the Commission undertook an investigation into the matter. The Commission's grounds of decision are set out below.

2 The Complainant alleged that she and her sisters had been receiving marketing calls and messages from various telemarketers (including moneylenders) on their mobile telephone numbers even though they had not consented to being contacted.

3 When the Complainant spoke to one of the telemarketers over the phone to ask where he had obtained her telephone number, she was informed that her name and telephone number were available on the Internet. This prompted the Complainant to conduct a search on the Internet for her name. Among the search results was a URL link ("Link") to the PropNex DNC List dated 29 July 2015 in PDF format.

4 The PropNex DNC List contained, amongst other things, the Complainant's full name, mobile number and landline, residential address and internal instructions to the Organisation agents regarding the Complainant.

MATERIAL FACTS AND DOCUMENTS

5 The Organisation is a real estate agency. P&N Holdings Pte Ltd ("P&N Holdings") is the parent company of the Organisation. Investigations disclosed that P&N Holdings and the Organisation share a common information technology ("IT") infrastructure. P&N Holdings maintains and operates the common IT infrastructure and provides IT support to the Organisation.

6 On 28 December 2015, the Commission was informed that the personal data of the 1,765 individuals contained in the PropNex DNC List were accessible to the public through the Link ("Data Breach Incident"). The PropNex DNC List was accessible to the public without authentication either through the Link or by performing an online search using search terms, for example, the Complainant's name, "PropNex" or the phrase "user files do not call". Investigations disclosed that the PropNex DNC List was disseminated internally as a PDF file that was uploaded onto the Organisation's virtual office system ("VO System"). For reasons detailed below, this PDF file was searchable and accessible on the Internet.

7 The PropNex DNC List included the following personal data:

(a) name;
(b) mobile number and/or landline;
(c) full or partial residential address;
(d) date of complaint by a particular individual;
(e) e-mail address; and
(f) internal instructions by the Organisation to its agents with regard to the individuals.

8 The Commission estimates that 96% or more of the records in the PropNex DNC List only contained a telephone number, residential address or e-mail address without any other identifying information.

9 On 31 December 2015, the Commission informed the Organisation's data protection officer of the Data Breach Incident and requested that the

PropNex DNC List be taken down. The Organisation confirmed that the PropNex DNC List belongs to the Organisation and that it had no knowledge of the Data Breach Incident until it was notified of the complaint. On 4 January 2016, the Organisation deleted the PropNex DNC List from its VO System and informed Google to exclude the Link from its search results. The Organisation also took steps to prevent a re-occurrence of the Data Breach Incident, by introducing a new way of disseminating the DNC List internally through a secured database and which can be searched using an authenticated web form.

10 Investigations disclosed that in or around July 2015, the PropNex DNC List was in PDF format and placed in a shared folder for internal use on the VO System which was accessible only by the Organisation agents and staff through authenticated login. Earlier versions of the PropNex DNC List had been placed in the same shared folder since the beginning of 2015.

11 The Organisation represented that it had put in place data protection policies, which were made known to its employees through briefings and addendums to their employment agreements. The Organisation also submitted that it had carried out penetration tests for its IT systems, and performed periodic searches on Google for possible leaked documents. In addition, the Organisation conducted security testing for web applications such as the VO System whenever major changes were conducted, and used "/robots.txt" to hide documents from Google's search engine crawler as well as to provide another layer of security for documents stored in the VO System.

12 However, the Organisation admitted that there was no password security whatsoever for the PropNex DNC List. The VO System's authentication only worked for web pages and not documents such as PDF files, which was the intended design and limitation of the original system. In relation to the shared folder in the VO System, this was meant for forms and templates and not "sensitive documents", but this policy was neither formally recorded nor communicated to users. Over time, therefore, this design limitation remained as a vulnerability but was overlooked.

13 According to the joint investigation carried out by the Organisation and P&N Holding, the Data Breach Incident was found to have occurred because the PropNex DNC List was indexed by Google and was therefore searchable and available on the Internet. This occurred despite the fact that

the PropNex DNC List was stored in a restricted web folder. This case demonstrates the weakness of relying on "/robots.txt" to hide the documents from the Google search engine crawler.

COMMISSION'S FINDINGS AND ASSESSMENT

14 At the outset, the Commission considers that the PropNex DNC List, containing amongst other things, individuals' names, contact numbers, residential addresses and e-mail addresses, does constitute personal data as defined in s 2(1) of the Personal Data Protection Act 2012[1] ("PDPA"). In addition, the Commission notes that the PropNex DNC List was an internal list maintained and stored on the Organisation's VO System. The Organisation does not dispute that the personal data in the PropNex DNC List contained personal data under the control of the Organisation at the material time.

15 Under s 24 of the PDPA, an organisation is obliged to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks ("Protection Obligation").

16 Accordingly, pursuant to s 24 of the PDPA, the Organisation is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to or of the PropNex DNC List.

Relationship between the Organisation and P&N Holdings and their obligations under the PDPA

17 Investigations disclosed that even though P&N Holdings and the Organisation shared a common IT infrastructure, with P&N Holdings maintaining and operating the common IT infrastructure and providing IT support to the Organisation, there was no evidence to suggest that P&N Holdings processed any personal data on behalf of the Organisation. Accordingly, the Commission does not consider that P&N Holdings is a data intermediary of the Organisation.

---

1 Act 26 of 2012.

Adequacy of security arrangements

18 After carefully considering all the relevant facts and representations made by the Organisation, the Commission is of the view that the Organisation failed to take reasonable security measures to protect the personal data in its possession and/or under its control. The Commission's reasons are set out below.

19 First, based on the Commission's investigations into the matter, the Commission finds that the VO System contained a significant system weakness, namely, that user authentication was only applied to web pages (*eg*, aspx files) but was not in place for document files (*eg*, PDF files). As a result of this weakness in the VO System, any user could have direct access to document files on the VO System, including the PropNex DNC List, by typing the Link in an Internet browser or through a Google search without having to go through any form of user authentication.

20 The Organisation was aware of this system weakness and it recognised that as a result of this system weakness, sensitive documents should not be placed on the VO System. However, the Organisation did not implement any security arrangements to militate against this known system weakness. For example, there was no policy to prohibit the sharing of sensitive documents on the VO System or to require that sensitive documents shared on the VO System be protected by a password.

21 Consequently, the PropNex DNC List was placed on the VO System as a PDF file without any password security or authentication, which in turn allowed the Data Breach Incident to occur and allowed various telemarketers to access and make use of the personal data in the PropNex DNC List.

22 Second, the Organisation's approach towards protecting the documents in the VO System through the use of "/robots.txt" was not sufficient and evinced an incorrect or inadequate understanding of the security measure which they chose to implement. The Organisation used "/robots.txt" in an attempt to hide the documents from the Google search engine crawler. The Organisation intended for this to be another layer of security for the documents stored in the VO System.

23 However, there are recognised weaknesses and limitations to relying on "/robots.txt" to hide the documents from the Google search engine crawler. For example, non-compliant (*eg*, malicious) web crawlers might

ignore the instructions in a "/robots.txt" file. The Organisation claims that it had only discovered these weaknesses and limitations after the Data Breach Incident. Contrary to the Organisation's claims, these weaknesses and limitations of "/robots.txt" are referred to in introductory articles such as the Google support article, "*Block URLs with robots.txt; Learn about robots.txt files*", which is easily accessible. The Organisation referred to this article in its representations, thereby showing that the Organisation could have and should have been aware of these weaknesses and limitations when they made use of this security measure.

24 The "/robots.txt" script was implemented to hide the web pages in the VO System from search engine crawlers; however, it cannot restrict or prevent access by external parties. Simply hiding a link to a document on the World Wide Web is not an effective way of ensuring that the document itself is protected from unauthorised access. The fact is that the document is still available online, and can be accessed by anyone over the World Wide Web. If the intent was to ensure that the document was for internal use, then appropriate restrictions and security measures should be placed to limit access to only the authorised persons.

25 Each organisation should adopt security arrangements that are reasonable and appropriate in the circumstances. If an organisation decides to use a particular security measure, it should be responsible for understanding the weaknesses and limitations (if any) of such a measure and to design and shape its security arrangements in light of those weaknesses and limitations.

26 It remains for the Commission to observe that the Organisation had implemented security arrangements and conducted periodic security testing. However, the Commission is of the view that the security arrangements and testing undertaken by the Organisation were insufficient to militate against the weaknesses in the VO System and to protect the personal data stored on the system. The technical limitations discussed above demonstrate this. Additionally, the Organisation had failed to discover the breach for a period that could extend to five months, from the time the PropNex DNC List was first placed in the VO System until a complaint was brought against it. This reinforces the Commission's finding that the security arrangements that had been implemented were insufficient to deter or to detect a data breach.

27 The Commission further finds that the corrective measures taken by the Organisation after the Data Breach Incident are only sufficient as an interim measure. Specifically, the Commission notes that following the Data Breach Incident, the Organisation had removed the PropNex DNC List from the VO System, and shifted it to a database which was accessible only through a new web application which required user authentication. However, the Organisation did not put in place any user authentication for document files stored in the VO System. Consequently, there is a risk that the Organisation's agents could continue to place unprotected document files containing personal data in the VO System, which would expose such personal data to the same risks as those arising from the Data Breach Incident, which could potentially result in other data breaches.

Exceptions under the Fourth Schedule to the PDPA

28 In its representations, the Organisation had indicated that it was relying on exceptions in paras 1(*a*) and 1(*h*) of the Fourth Schedule to the PDPA. However, the Organisation did not explain how the foregoing exceptions would apply in respect of the Protection Obligation. Nonetheless, the Commission considered the potential application of these exceptions. In its deliberations, it was not apparent how the Organisation's disclosure of the PropNex DNC List "is necessary for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way"[2] or "is necessary for evaluative purposes".[3] Accordingly, the Commission considers that the Organisation's reliance on the exceptions to the Consent Obligation in paras 1(*a*) and 1(*h*) of the Fourth Schedule to the PDPA is irrelevant to this case, and without merit.

ENFORCEMENT ACTION BY THE COMMISSION

29 Having completed its investigation and assessment of this matter, the Commission finds that in light of the weakness in the VO System and the

2 Personal Data Protection Act 2012 (Act 26 of 2012) Fourth Schedule, para 1(*a*).

3 Personal Data Protection Act 2012 (Act 26 of 2012) Fourth Schedule, para 1(*h*).

failure to implement security arrangements which would militate against the known VO System weaknesses, the Organisation failed to take reasonable security measures to protect the personal data in its possession and/or under its control and is in breach of s 24 of the PDPA.

30 In exercise of the power conferred upon the Commission pursuant to s 29 of the PDPA, the Commission directs that a financial penalty of $10,000 be imposed on the Organisation.

31 During the course of investigations, the Organisation represented that the VO System was not intended to be used for the storage or sharing of documents containing personal data. However, the Commission notes that the VO System is a system that is meant for the online sharing of documents between the Organisation agents and/or employees through the Internet. This being the case, it is foreseeable that some of the documents stored and/or shared on this system may contain personal data. The Commission therefore additionally directs that the Organisation:

(a) ceases the storage and/or sharing of documents containing personal data using the VO System until the design flaw of the VO System has been fixed; and

(b) conducts a security scan on the VO System to identify and fix any additional vulnerabilities before it is made accessible online.

32 In assessing the breach and the directions to be imposed, the Commission took into account the following factors:

(a) the Data Breach Incident involved 1,765 individuals and their personal data were disclosed to the public;

(b) the Data Breach Incident was caused by a flaw in the Organisation's VO System;

(c) the Organisation admitted to the Data Breach Incident in the first instance;

(d) 96% or more of the records concerning the 1,756 individuals contained either a telephone number, residential address or e-mail address without any other personal data;

(e) the Organisation took prompt remedial actions to rectify and prevent the recurrence of the data breach;

(f) the Organisation had been co-operative and forthcoming during the investigations;

(g) the Organisation did have in place a data protection policy which they made known to their agents and staff; and

(h) the Organisation's in-house compliance team (with the assistance of external consultants, where necessary) did conduct annual internal audits to assess:

(i) system access risk;

(ii) data integrity risk; and

(iii) risk of configuration issues in production environment.

33 The Commission emphasises that it takes a very serious view of any instance of non-compliance under 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.

YEONG ZEE KIN
Deputy Commissioner
Personal Data Protection Commission

Grounds of Decision

Re JP Pepperdine Group Pte Ltd

Case Number: DP-1510-A558
Decision Citation: [2017] SGPDPC 2

Protection Obligation *– Disclosure of personal data – Insufficient technical security arrangements*

25 January 2017

BACKGROUND

1 On 25 October 2015, the Complainant informed the Personal Data Protection Commission ("Commission") that any member of the public could readily access the personal data of members that had joined the Organisation's membership programme by:

(a) entering a randomly simulated membership number on a web page (<http://goo.gl/5BX9Rr>, a Google URL Shortener that redirects to <http://ascentis.com.sg/microcrm/JacksPlace_memberportal/searchprofile.aspx>) listed on the Organisation's membership brochure ("Web Page"); or

(b) performing a search (without inputting any search parameters) using the search functions available on the Web Page.

2 On account of the complaints made, the Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether the Organisation had breached its obligations under the PDPA. The material facts of the case are as follows.

MATERIAL FACTS AND DOCUMENTS

3 The Organisation operates a number of restaurants in Singapore under various brands (*eg*, Jack's Place, Eatzi Gourmet). The Organisation

1 Act 26 of 2012.

has a membership programme for its customers. Participating in the membership programme entitles members to special promotions and discounts across the different restaurants operated by the Organisation.

4 Each member would be assigned a 7-digit membership number by the Organisation. Membership numbers run sequentially. At the time of the investigation (December 2015), the Organisation had approximately 30,000 members.

5 As part of the investigation, the Commission verified that personal data of members of the Organisation's membership programme were publicly accessible through the Web Page by:

(a) entering a randomly simulated membership number in the search facility on the Web Page, which would retrieve membership details associated with that account; or

(b) simply clicking on the "Search" button in the search facility without any search parameters, *ie*, the search fields were left blank, which would randomly retrieve the details of a membership account.

6 The personal data that were publicly accessible through the Web Page included names of members, gender, marital status, nationality, race, NRIC/Passport number, date of birth, mobile phone number, home phone number, e-mail addresses, residential addresses and other membership account details.

7 The material facts from the Commission's investigations are as follows:

(a) The Web Page was developed for the purposes of a one-off promotional event held in the first half of 2013 to recruit new members and to encourage existing members to update their personal particulars. The Web Page was created by the Organisation's vendor, Ascentis Pte Ltd ("Ascentis"). The Web Page contained a search facility that enabled searches and retrieval of personal particulars of the members of the Organisation's membership programme.

(b) The Organisation claims that the Web Page was intended for internal use, and for the Organisation's staff to remotely search and access the Organisation's member database. Although the Web Page was not intended for public access, the Organisation did not put in place security measures (or require Ascentis to design any security measures) to control access and ensure that the Web Page was

inaccessible to the public. The Web Page was not removed after the end of the promotional event in 2013 and remained accessible to both staff and the public until 29 October 2015.

(c) The Organisation listed in its membership brochures a hyperlink that was truncated using a Google URL shortening service ("a Google URL Shortener") that redirected any person who accessed it to the Web Page. These membership brochures, which contained the Google URL Shortener and other information on the membership application process, were disseminated by the Organisation to all the restaurants under its different brands. The Organisation claims that the redirection to the Web Page was a mistake and that the public should have been redirected to the Organisation's membership portal located at another URL. Yet, for the entire period the membership brochure was in circulation at the Organisation's restaurants (from as early as 2013), the URL listed in the brochures had not been corrected.

(d) The Web Page had a security loophole, as described above at [5(b)], that caused the random retrieval of members' account details whenever the "Search" button was clicked with no search parameters. The Organisation admitted that the loophole was caused by an unpatched bug in the original version of the Web Page. The Organisation was not aware of the existence of the bug in the Web Page or the resulting security loophole until it was notified by the Commission.

8 On 29 October 2015, after receiving the Commission's notification, the Organisation introduced security features to the Web Page by incorporating a password protection feature such that the Web Page was no longer publicly accessible and could only be accessed after authentication.

9 Subsequently, the Organisation implemented further measures to address the complaint:

(a) the Organisation secured the Web Page with a landing page which was password-protected. Access to the Web Page would only be granted through inputting user credentials known only to the Web Page's administrators; and

(b) the Organisation also took steps to ensure that all references to the Google URL Shortener listed in the Organisation's membership brochures that were still available in the Organisation's restaurants were removed.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Issue to be determined

10 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

11 The issue in the present case is whether the Organisation had breached s 24 of the PDPA, when personal data (of members of the Organisation's membership programme) could be accessed on the Web Page (in the manner described at [5] above).

Whether the Organisation had complied with section 24

12 The data accessible on the Web Page included the names of members of the Organisation's membership programme, their contact information, addresses and identification numbers. These data fall within the definition of "personal data" under the PDPA.

13 The personal data accessible on the Web Page were also under the control of the Organisation. The Organisation demonstrated this control when it was able to promptly effect changes to the Web Page to restrict public access to such personal data when contacted by the Commission.

14 In the course of investigations, Ascentis confirmed that the Web Page was designed without any security measures as *per* the Organisation's specifications. The Organisation claims that it did not require security features to be incorporated because the Web Page was intended for (a) internal (and not public) purposes; and (b) temporary use at the Organisation's 2013 promotional event.

15 This may have been the state of the Organisation's system in 2013; but when the PDPA came into full effect on 2 July 2014, it was incumbent on the Organisation to ensure that it had in place the necessary security arrangements to protect the data. Steps must be taken to ensure that the security that would protect the personal data under the Organisation's possession or control was ready by the time that the PDPA had come into full force. In the Commission's view, one of the first few steps that ought to have been taken was to determine if the system was to continue to be made

accessible via the Internet or to keep it wholly within its internal network. Thereafter, the Organisation ought to have conducted a review of its system so as to determine the weakness and vulnerabilities of the system for the type of access and use that was intended. This would allow the Organisation to know where the weaknesses and vulnerabilities are which needed to be addressed.

16 In this case, the loophole in the Web Page was a significant gap in the protection of the system that allowed unauthorised access to personal data stored on the server. The Organisation had not shown that it took any steps (as mentioned at [15] above) to detect and rectify this problem. No checks or tests were done on the system. No steps were taken to ascertain and limit (or block) the entry points to the personal data stored on the server. Indeed, the Web Page proved to be one such entry point. The Organisation failed to have the Web Page taken down, notwithstanding that the Organisation had, from the outset, intended to do so. In this regard, the Organisation did not ensure the security of the personal data it was obliged to protect.

17 It is clear that the Organisation's system did not have any reasonable or adequate security arrangements to protect the personal data that were accessible through the Web Page:

(a) There were no security or access controls to the Web Page and any member of the public could have accessed the personal data of the Organisation's members through the Web Page. Even if the Web Page was intended by the Organisation to be for internal use, there would still be an obligation on the Organisation to make reasonable security arrangements to prevent unauthorised access to the personal data stored on the system. In the present case, knowing that the personal data was stored online and could be accessed from the Web Page, the Organisation should have at least implemented basic technical security measures to ensure that the system, including the Web Page, was secure and not accessible by the public.

(b) The Web Page allowed the use of the membership number assigned to each member to serve the functions of identification and authentication to access personal data. In the Commission's view, where a single string of numbers is the only security arrangement serving both to identify and authenticate access to personal data, such security arrangement could be considered reasonable only if (depending on the sensitivity of the personal data being protected) this number was

unique, unpredictable and reasonably well protected. In this case, the membership numbers assigned by the Organisation to its members were issued in running sequence and easy to ascertain or deduce, and therefore, such a security arrangement could not be considered reasonable.

(c) The Web Page contained a security loophole (described at [5] above) which effectively allowed members of the public free and unfettered access to personal data of random account holders through the Web Page.

18 Additionally, by including the Google URL Shortener in the brochure, which redirected a person to the Web Page, the Organisation was facilitating access to the Web Page, and the personal data held on the system. A user that followed the link would, whether by accident or on purpose, be able to gain access to the personal data of the Organisation's customers. While the Organisation submits that the redirection of the link was wrong and unintended, the Commission does not find this to be excusable. A prudent organisation which was promulgating a link to the public should at least check the link before publication. Had the Organisation done so, it would have noticed that there was something amiss, as the link would have brought up the Web Page, which was not supposed to be in operation.

19 In view of the above, the Commission finds that the Organisation had failed to make reasonable security arrangements to protect personal data in its possession or under its control. As such, the Organisation was in breach of s 24 of the PDPA.

20 The Commission adds that although the Web Page was designed by Ascentis, on the available facts, Ascentis was not a data intermediary for the Organisation. There is no evidence that Ascentis processed any personal data on behalf of the Organisation. Ascentis's role was limited to designing the Web Page for the Organisation according to the instructions of the Organisation. Accordingly, the Commission makes no findings in respect of Ascentis.

ACTIONS TAKEN BY THE COMMISSION

21 Given the Commission's findings that the Organisation is in breach of its obligations under s 24 of the PDPA, the Commission is empowered

under s 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 $1m.

22 In determining the direction, if any, to be made, the Commission considered the following factors related to the case, including the mitigating and aggravating factors set out below:

(a) A substantial amount of personal data of some 30,000 members of the Organisation's membership programme was placed at risk. This risk was exacerbated by the Organisation's publication of the Google URL Shortener, which redirected individuals to the Web Page with the security loophole, in its membership brochures that were disseminated to all its restaurants.

(b) The personal data at risk involved sensitive personal data such as the NRIC/Passport numbers of members of the Organisation's membership programme.

(c) The data breach may have been avoided (or the impact of the breach reduced) if the Organisation had taken the following simple steps:

(i) reviewing the information in its own membership brochures, at which point it would have realised that members of the public were being mistakenly redirected to the Web Page (intended for internal use) instead of the Organisation's membership portal; and/or

(ii) ensuring that the Web Page (intended for internal use) was inaccessible to the public right from the outset, or by promptly removing the Web Page once the 2013 promotional event for which the Web Page was created had concluded.

(d) The Organisation took prompt action to remedy the breach when notified by the Commission.

23 In view of the factors noted above, pursuant to s 29(2) of the PDPA, the Commission hereby directs that the Organisation pay a financial penalty of $10,000 within 30 days of the Commission's direction, failing which interest at the rate specified in the Rules of Court[2] in respect of

2 Cap 322, R 5, 2014 Rev Ed.

judgment debts shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
Deputy Commissioner
Personal Data Protection Commission

Grounds of Decision

Re Executive Coach International Pte Ltd

Case Number: DP-1504-A426
Decision Citation: [2017] SGPDPC 3

Consent Obligation *– Disclosure of personal data without consent*
Liability of employers for acts of employees
Notification Obligation *– Disclosure of personal data without notification*

21 March 2017

BACKGROUND

1 On 20 April 2015, the Complainant complained to the Personal Data Protection Commission ("Commission") that the Organisation had disclosed her past personal history in a WhatsApp group chat comprising the Complainant and the Organisation's other staff and volunteer trainees ("WhatsApp Group") without her consent and without notifying her of the purposes for the disclosure.

2 On account of the complaint made, the Commission commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] ("PDPA") to ascertain whether the Organisation had breached its obligations under the PDPA. The material facts of the case are as follows.

MATERIAL FACTS AND DOCUMENTS

3 The Organisation is an organisation which provides life and executive coaching services to individual and corporate clients. The Complainant is a former employee of the Organisation. She was the personal assistant to [redacted] ("Mr L"), a director of the Organisation. The Complainant has since left the employment of the Organisation on unamicable terms.

1 Act 26 of 2012.

4 The WhatsApp Group, comprising of the Organisation's employees and volunteers, was created on 22 August 2013. The Complainant and Mr L were both participants in this WhatsApp Group. At the material time on 7 April 2015, there were a number of other participants in this WhatsApp Group.[2]

5 On 7 April 2015, Mr L disclosed highly sensitive information of the Complainant's personal history, namely her past drug problem and issue with infidelity in her amorous relationship ("Personal Data"), to the participants in the WhatsApp Group. The Organisation has not disputed that the personal history of the Complainant is personal data. The disclosure of the Personal Data was made by Mr L following allegations that she was undermining the Organisation's authority by persuading the employees and volunteers of the Organisation to leave the Organisation.

6 The Complainant claims that the Personal Data was disclosed by her to Mr L in the context of Mr L being the Complainant's employer, teacher and coach.

7 On 11 May 2015, the Commission notified the Organisation of the complaint and requested the Organisation to co-operate and assist in investigations. In the course of the investigations, the Organisation represented to the Commission that:

2 The Complainant and Organisation disagreed on the exact number of participants in the WhatsApp Group on 7 April 2015. The Complainant claimed that the WhatsApp Group contained 117 participants. The Organisation claimed that there were only 58 participants and that a group could only accommodate a maximum of 100 participants. The Commission does not have sufficient evidence to decide on the *exact* number of participants. However, the exact number of participants is immaterial in this case and the Commission will accept that there were at least 58 participants in the WhatsApp Group on 7 April 2015.

(a) Mr L disclosed the Personal Data in his personal capacity and not as an employee of the Organisation; and

(b) the Personal Data was only known to Mr L and not the Organisation, and that the Organisation did not authorise Mr L to disclose the Personal Data.

COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

Issues to be determined

8 The issues to be determined in the present case are as follows:

(a) Whether the Organisation is responsible for Mr L's disclosure of the Personal Data.

(b) If the Organisation is liable for Mr L's disclosure, whether the Organisation is in breach of ss 13 and 20 of the PDPA for the said disclosure.

Whether the Organisation is responsible for Mr L's disclosure of the Personal Data

9 The Personal Data disclosed involved sensitive data of the Complainant's personal history, and in this instance, there is no question, and it is not disputed, that such information falls within the definition of "personal data" under the PDPA. The nature of the Personal Data, including the fact that the Complainant was identified in the WhatsApp Group, puts it beyond doubt that the information was information "about an individual who can be identified from that data".

10 Under s 53(1) of the PDPA, any acts done or conduct engaged in by an *employee in the course of his employment* shall be treated for the purposes of the PDPA as done or engaged in by his employer as well as him, *whether or not it was done or engaged in with the employer's knowledge or approval*.

11 Based on the facts described at [3] to [7] above, the Commission notes that the disclosure of the Personal Data was made in the context of an ongoing dispute arising from the unamicable departure of the Complainant from the Organisation's employment. The Organisation's director, Mr L, had expressed his disappointment and views with the Complainant in the WhatsApp Group chat following her resignation from the Organisation,

and claimed that the Complainant had subsequently sought to undermine his authority, and to persuade the Organisation's employees and volunteers to leave the organisation. The Complainant, on the other hand, had expressed her own disappointment with Mr L's conduct (personally, and as an employer, teacher and coach) and raised issues that she had with the Organisation during her time of employment. Against this background, the disclosure of the Personal Data in the WhatsApp Group was not made by parties in the personal sense, but was made *viz* an ongoing dispute between an employer and its ex-employee, with the intent to discredit the ex-employee. Accordingly, the Commission is of the view that Mr L was acting in the course of his employment as a director of the Organisation when he disclosed the Complainant's Personal Data in the WhatsApp Group chat, and was not, as the Organisation claims, disclosed by Mr L acting in his individual capacity.

12 The Organisation claims that it did not know or approve of Mr L's collection and disclosure of the Personal Data. Even if this is true, the Organisation's knowledge or approval is immaterial under s 53(1) of the PDPA. It is noted that Mr L was at all material times a senior member of the Organisation.

13 Accordingly, pursuant to s 53(1) of the PDPA, because Mr L's disclosure of the Personal Data was made in the course of employment, the disclosure is treated as a disclosure by the Organisation, for which the Organisation is responsible.

Whether the Organisation is in breach of sections 13 and 20 of the PDPA for the said disclosure

14 Section 13 of the PDPA prohibits organisations from collecting, using or disclosing personal data about an individual unless:

> (a) the individual gives, or is deemed to have given, consent under the PDPA to such collection, use or disclosure; or
>
> (b) the collection, use or disclosure of the personal data without the individual's consent is required or authorised under the PDPA or any written law.

15 Section 20 of the PDPA requires, amongst other things, that an organisation informs an individual of:

> (a) the purposes for the collection, use or disclosure of personal data, on or before collecting the personal data; and
> (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a) above before the use or disclosure of the personal data for that purpose.

16 In the present case, there is no dispute that neither Mr L nor the Organisation obtained the Complainant's consent or informed the Complainant of the purposes of the disclosure, before disclosing the Personal Data. The Organisation has not referred to any of the exceptions in the Fourth Schedule to the PDPA in its response and the Commission also takes the view that none of the exceptions apply in the present case.

17 Accordingly, the Commission finds the Organisation in breach of ss 13 and 20 of the PDPA.

ACTIONS TAKEN BY THE COMMISSION

18 Given the Commission's findings that the Organisation is in breach of its obligations under ss 13 and 20 of the PDPA, the Commission is empowered under s 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 $1m.

19 The Commission notes that the disclosure was deliberately made, and under circumstances to discredit the Complainant. The Personal Data that was disclosed was also highly sensitive. However, the Commission is also mindful of the fact that the disclosure was made in the context of a dispute between an employer and ex-employee, and made in what essentially was the Organisation's chat group for work (and not to the public at large). On balance, therefore, even though the Commission has found the Organisation to be in breach of ss 13 and 20 of the PDPA, the Commission is of the view that the enforcement action to be taken in this case should be calibrated based on the circumstances of the case.

20 Accordingly, the Commission has decided not to issue any direction to the Organisation to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning to the Organisation for the breach of its obligations under ss 13 and 20 of the PDPA.

YEONG ZEE KIN
Deputy Commissioner
Personal Data Protection Commission

Case Summary

RE ADVENT LAW CORPORATION

Application of other written laws *– Rules of Court (Cap 322, R 5, 2014 Rev Ed)*
Protection Obligation *– Disclosure of personal data*

29 December 2015

BACKGROUND

1 The Organisation is a law firm. Its client(s) had commenced a civil action against the Complainant and the Organisation had sought to effect service of the writ of summons on the Complainant by leaving the writ at the front gate of the Complainant's residence. The Complainant complained that this manner of service exposed the contents of the document to passers-by. The Complainant alleged that a passer-by could view his personal data contained in the document, such as his full name, National Registration Identity Card number, and the sum claimed against the Complainant. The Complainant claimed, therefore, that the Organisation had failed to protect his personal data from unauthorised access or disclosure.

ISSUE

2 The Organisation had produced evidence to show that the manner of substituted service of the writ of summons was done in accordance with the Rules of Court[1] ("Rules of Court"). The issue is whether the Organisation could effect substituted service in accordance with the Rules of Court.

1 Cap 322, R 5, 2014 Rev Ed.

FINDINGS

3 Section 4(6)(*b*) of the Personal Data Protection Act 2012[2] ("PDPA") provides that the provisions of the other written laws shall prevail to the extent that any provision of Pts III to VI of the PDPA ("Data Protection Provisions") is inconsistent with the provisions of that other written law. The Rules of Court is subsidiary legislation made under the Supreme Court of Judicature Act (Cap 322), and therefore fall within the meaning of "written law" in s 4(6) of the PDPA. Hence, the Data Protection Provisions are subordinate to the Rules of Court. Since the manner of substituted service by the Organisation is provided for in the Rules of Court, the PDPA does not prevent the Organisation from effecting substituted service in the manner ordered by the court in exercise of its powers under the Rules of Court. Accordingly, the Personal Data Protection Commission found the Organisation not to be in breach of the PDPA.

---

2 Act 26 of 2012.

Case Summary

RE UNITED OVERSEAS BANK GROUP

Accuracy Obligation *– Last known contact information provided by account holder was accurate – Account holder did not inform Organisation of change in contact information*

13 January 2016

BACKGROUND

1 The Organisation is a bank, and the Complainant, an individual. The complaint concerned several SMS messages that the Complainant had received from the Organisation on his prepaid mobile phone. The SMS messages contained one-time passwords ("OTP") that were issued by the bank. The Complainant received the SMS messages even though he did not make any transactions with his bank account.

2 The Organisation informed the Personal Data Protection Commission that the OTPs were meant for another account holder who had not updated his contact information with the bank. The Complainant had received the OTPs because he had been assigned the recycled mobile number that previously belonged to the account holder.

ISSUE

3 Given that the mobile number which the Organisation had sent the Complainant the SMS messages to was not up-to-date, the issue is whether the Organisation had complied with its Accuracy Obligation.[1]

FINDINGS

4 Since the account holder did not inform the Organisation that he had changed his contact information, it was not possible for the Organisation to

1 Pursuant to s 23 of the Personal Data Protection Act 2012 (Act 26 of 2012).

have known that the contact information was no longer valid. At the time the OTPs were sent, the last known contact information provided by the account holder was accurate. Accordingly, even though the contact information it retained was no longer accurate, the Commission found that the Organisation was not in breach of s 23 of the Personal Data Protection Act 2012.[2]

2 Act 26 of 2012.

Case Summary

RE SINGAPORE INSTITUTE OF MANAGEMENT PTE LTD

Protection Obligation *– Administrative and technical security arrangements*

29 January 2016

BACKGROUND

1 The complaint concerned the alleged disclosure of the Complainant's personal data by the Organisation to a third party via the Organisation's online portal ("Portal").

2 In February 2014, the Complainant and the third party submitted their applications for the Organisation's diploma programme. While processing their applications, a staff of the Organisation erroneously uploaded the Complainant's scanned National Registration Identity Card ("NRIC") image to the third party's online application records. This human error resulted in the disclosure of the Complainant's personal data to the third party when the latter sought to access his online application records via the Portal in September 2016. No other person besides the third party was able to view the Complainant's personal data on the Portal.

3 When the Complainant notified the Organisation, it removed the Complainant's scanned NRIC image from the third party's online application records and advised the latter to delete the erroneous application form containing the Complainant's scanned NRIC image. The staff who committed the error had also been counselled.

ISSUE

4 The key issue is whether the Organisation had made reasonable security arrangements to protect the Complainant's personal data, pursuant to the Protection Obligation.[1]

1 Pursuant to s 24 of the Personal Data Protection Act 2012 (Act 26 of 2012).

FINDINGS

5 Although the error occurred before the relevant data protection obligations under the Personal Data Protection Act 2012[2] ("PDPA") came into force on 2 July 2014 ("effective date"), the Organisation had a continuing obligation to protect the Complainant's personal data from unauthorised disclosure because it had possession and control of the Complainant's past application records even after the effective date.

6 In this regard, the Personal Data Protection Commission determined that the sample documentary checks that the Organisation instituted at the material time were adequate in providing reasonable assurance of the correct tagging of applicants' scanned documents. While a complete check could have possibly detected the error, the Commission takes the pragmatic view that this would have been overly onerous, considering the Organisation's high application processing volume and the low risk of such an error occurring.

7 Having evaluated the facts and circumstances, the Commission was satisfied that the Organisation had adequately discharged its Protection Obligation.

8 The Organisation nevertheless subsequently tightened its internal procedures for validating online applicants' records and did away with the display of images of scanned documents on the Portal to prevent future errors. However, the Commission is of the view that the latter measure may not be necessary for compliance with the PDPA, not least since it serves a useful function of allowing users to verify their personal data.

---

2 Act 26 of 2012.

Case Summary

RE ASIA RENAL CARE (KATONG) PTE LTD AND ANOTHER

Consent Obligation *– Disclosure of personal data – Whether there was deemed consent when personal data was used to respond to Complainant's complaint*

1 February 2016

BACKGROUND

1 The Complainant was a dialysis patient for a number of years at a clinic operated by the First Organisation. The Second Organisation is the majority shareholder of the First Organisation.

2 On 8 June 2015, the managing director and operations manager of the Second Organisation delivered a letter to the Complainant. The letter concerned the complaints that the Complainant had with the service he received at the clinic, but it also addressed the Complainant's combative behaviour towards the staff, nurses, doctors and other patients at the clinic. As the Second Organisation was of the view that such behaviour was disruptive to the operations of the clinic, it raised the possibility of termination of the clinic's services to the Complainant in the letter.

3 The Complainant's name and residential address was set out as the addressee at the top of the letter. The Complainant lodged a complaint with the Commission, alleging that there was an unauthorised collection and use of his personal data by the Second Organisation without his consent. The Complainant further alleged that the First Organisation ought not to have disclosed his personal data to the Second Organisation.

ISSUE

4 The first issue was whether the Complainant consented to, or could be deemed to have consented to, the Second Organisation collecting and

using his personal data for the purposes of sending him the letter in question, pursuant to the Consent Obligation.[1]

5 The second issue was whether the First Organisation is permitted to disclose the Complainant's personal data to the Second Organisation pursuant to the Consent Obligation.[2]

FINDINGS

6 The Commission found that the Complainant had, before his receipt of the letter in question, already been raising complaints about the service at the clinic directly to the Second Organisation and, on occasion, to both Organisations simultaneously. Additionally, while corresponding with the Second Organisation, the Complainant had provided his contact details to the Second Organisation directly.

7 By such actions, the Complainant must be taken to have consented or be deemed to have consented to the Second Organisation's use of the Complainant's personal data for the purposes of engaging with him over the issues he raised and on the subject matter of his complaints, *ie*, his service experience at the clinic.

8 Accordingly, the Commission found that the First and Second Organisations did not breach their Consent Obligations under the Personal Data Protection Act 2012.[3]

---

1 Pursuant to ss 13 to 15 of the Personal Data Protection Act 2012 (Act 26 of 2012).

2 Pursuant to ss 13 and 14 of the Personal Data Protection Act 2012 (Act 26 of 2012).

3 Act 26 of 2012.

Case Summary

RE DBS BANK LTD

Consent Obligation *– Disclosure of personal data – Personal data shared within business units in Organisation*

4 February 2016

BACKGROUND

1 The Complainant is an existing customer of the Organisation, a bank with several business units.

2 The Complainant had previously provided his personal mobile phone number to a representative of Unit 1 of the Organisation in connection with a matter relating to his personal bank account. Subsequently, the Complainant received a call made to his personal mobile phone number from a representative of Unit 2 of the Organisation in connection with a separate business matter concerning a proposed investment fund.

3 In his complaint to the Personal Data Protection Commission, the Complainant alleged that the representative of Unit 1 had disclosed his personal mobile phone number without his consent to a representative of Unit 2, and that the representative of Unit 2 had used his number to contact him without his consent.

ISSUE

4 The main issue in this case is whether the stated use and disclosure of the Complainant's personal mobile phone number were in compliance with the Organisation's Consent Obligation.[1]

1 Pursuant to ss 13 and 14 of the Personal Data Protection Act 2012 (Act 26 of 2012).

FINDINGS

5 The Organisation confirmed that both Units 1 and 2 are business units under the same Organisation and therefore part of the same legal entity. Unit 1 is a customer unit of the Organisation providing a safekeeping service, whereas Unit 2 is the Organisation's corporate banking business. Given that Units 1 and 2 are business units that are part of the same Organisation and not separate "organisations", the use and disclosure of the Complainant's phone number by Units 1 and 2 did not amount to an unauthorised use or disclosure of personal data by the Organisation.

6 Moreover, investigations revealed that the Complainant had made some queries on a real estate investment trust during correspondence with a representative of Unit 1, resulting in that representative of Unit 1 handing the Complainant's queries over to his business banking colleagues from Unit 2 of the Organisation for follow up handling.

7 Investigations also disclosed that the Complainant had been equivocal in his instructions to the Organisation pertaining to the use of his personal mobile phone number. On some occasions, he intimated that he did not wish to use his personal mobile phone number to discuss a proposed investment fund, requesting to correspond via e-mail instead. On other occasions, he scheduled conference calls with the representatives of Unit 2 to discuss the same fund using his personal mobile phone number.

8 As there was insufficient evidence to support the complaint, investigations were discontinued.

Case Summary

RE SAVILLS RESIDENTIAL PTE LTD

Consent Obligation *– Use or disclosure of personal data – Insufficient clarity on purpose for use or disclosure of personal data*

17 February 2016

BACKGROUND

1 The Complainant brought a complaint against the Organisation alleging that her personal data, specifically her residential address at the time, had been disclosed to a third party without her consent. The Organisation is an individual carrying on business as a registered salesperson engaged by a property agency. The Complainant and her family were formerly tenants of one of the Organisation's clients.

2 Upon the expiry of the tenancy, the Complainant moved out of the tenanted property ("Tenanted Property") and into her parents' place. The Complainant disclosed her parents' address to the Organisation but contended that she had only done so in order for her mail to be forwarded to her parents' address.

3 Shortly after the Complainant moved out, debt collectors looking for repayment from the Complainant's husband started harassing the new tenants at the Tenanted Property. In order to stop the debt collectors from harassing the new tenants, the Organisation informed the debt collectors that the Complainant and her family had moved out and disclosed to them the Complainant's residential address at the time, *ie*, the Complainant's parents' address.

ISSUE

4 The key issue is whether the Organisation's disclosure of the Complainant's personal data to the debt collectors was in compliance with its Consent Obligation.[1]

FINDINGS

5 In this case, neither party was able to produce any documents evincing the parties' understanding or agreement regarding the purposes for which the Complainant provided her new residential address to the Organisation. There was no evidence to corroborate the Complainant's assertion that she had provided her new residential address to the Organisation for the sole purpose of forwarding her mail. Neither could the Organisation produce evidence to corroborate its claim that the Complainant had provided her new residential address for a more general and open-ended purpose. Consequently, it was not apparent to the Personal Data Protection Commission what the boundaries of the consent were and therefore whether the Organisation exceeded those boundaries by disclosing the Complainant's new residential address to the debt collectors.

6 As the Commission was unable to make out a clear case of breach against the Organisation, an advisory notice was issued to the Organisation.

---

1 Pursuant to ss 13 and 14 of the Personal Data Protection Act 2012 (Act 26 of 2012).

Case Summary

RE SELBY JENNINGS, A TRADING STYLE OF PHAIDON INTERNATIONAL (SINGAPORE) PTE LTD

Consent Obligation *– Use of personal data without consent – Whether publicly available exception applicable*

25 February 2016

BACKGROUND

1 The Organisation is the Singapore subsidiary of a foreign recruitment company which specialises in the banking and financial services industry. The Complainant is listed as a candidate in the Organisation's database.

2 Prior to the incident, the Complainant had uploaded his curriculum vitae ("CV") containing his contact details on the online platform eFinancial. The Complainant's CV and contact details were publicly available through this platform at the material time.

3 On 13 January 2015, the Organisation contacted the Complainant via e-mail to offer him an employment opportunity. The Complainant instructed the Organisation to remove his CV and contact details from its database as he did not wish to be contacted about further employment opportunities. However, an employee of the Organisation had overlooked the Complainant's request and failed to remove him from the mailing list. Due to this oversight, the Organisation subsequently contacted the Complainant again on two occasions via e-mail and telephone to offer him employment opportunities.

4 The Complainant filed a complaint with the Personal Data Protection Commission concerning the Organisation's unauthorised collection and use of his personal data, and the Organisation's continued use even after he had expressly withdrawn his consent.

ISSUE

5 There are two main issues in this case. The first issue is whether the Organisation collected and used the personal data of the Complainant without his consent in breach of its Consent Obligation.[1] The second issue is whether the Organisation continued to use the personal data of the Complainant even after the Complainant had withdrawn his consent.[2]

6 Subject to exceptions, an organisation is prohibited from collecting or using an individual's personal data unless the individual gives, or is deemed to have given, his consent for the collection or use of personal data.[3] One such exception is the publicly available exception, as found in the Second, Third and Fourth Schedules to the Personal Data Protection Act 2012[4] ("PDPA").

7 As to the issue of withdrawal of consent, s 16 of the PDPA provides that an individual may, upon giving reasonable notice to the organisation, at any time withdraw any consent given, or deemed to have been given, under the PDPA.

FINDINGS

8 Concerning the first issue, the Organisation was found not to be in breach of its Consent Obligation under the PDPA as the publicly available exception was applicable. The Complainant's CV and contact details were publicly available on the online platform eFinancial throughout the material time, and there were no restrictions placed on any user or recruitment company from accessing the information on eFinancial.

9 In the Commission's view, in so far as the personal data in question was publicly available at the point of collection, the Organisation would be able to use and disclose personal data without the Complainant's consent,

---

1 Pursuant to ss 13 and 14 of the Personal Data Protection Act 2012 (Act 26 of 2012).

2 Pursuant to s 16 of the Personal Data Protection Act 2012 (Act 26 of 2012).

3 Pursuant to ss 13 to 15 of the Personal Data Protection Act 2012 (Act 26 of 2012).

4 Act 26 of 2012.

notwithstanding that the personal data may no longer be publicly available at the point in time when it was actually used or disclosed.[5]

10 With regard to the second issue, the Commission decided that the Complainant's attempt to withdraw any consent he may have given for the Organisation to contact him with employment opportunities was ineffective since there was no requirement to obtain consent in the first place. Further, his CV was still publicly available at the material time. Thus, there was no need for the Organisation to obtain consent at the outset.

11 Accordingly, the Organisation was not in breach of its Consent Obligations under the PDPA.

---

5 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at para 12.61.

Case Summary

RE STRATAGEM GLOBAL RECRUITMENT PTE LTD

Consent Obligation *– Use of personal data without consent – Whether publicly available exception applicable*

25 February 2016

BACKGROUND

1 The Organisation is a boutique job search consultancy agency. The Complainant was registered with the Organisation as a job seeker and received information about employment opportunities. After a few years, the Complainant notified the Organisation that he no longer wished to receive its services. Notwithstanding this, the Complainant continued to received e-mails on potential employment opportunities from the Organisation.

2 Investigations disclosed that the Organisation had removed the Complainant's personal data from its database. Due to a technical glitch, the Organisation had to rely on its backup database which had not been updated. Consequently, the Organisation continued to send e-mails to the Complainant because his personal data was still in its backup database.

ISSUE

3 The issues are (a) whether the Organisation breached its Consent Obligation,[1] and (b) whether any exceptions under the Personal Data Protection Act 2012[2] ("PDPA") in the Fourth Schedule applied. One such exception is where the personal data disclosed is publicly available.

1 Pursuant to ss 13 and 14 of the Personal Data Protection Act 2012 (Act 26 of 2012).

2 Act 26 of 2012.

FINDINGS

4 Investigations disclosed that after he had ceased using the Organisation's job search consultancy services, the Complainant was registered with another job search platform and his curriculum vitae ("CV") containing his personal data was publicly available at the time the e-mails were sent to him.

5 The Personal Data Protection Commission decided that so long as the personal data in question was publicly available at the time of collection, use or disclosure (as the case may be), the source of the personal data did not change the fact that no consent was required for the Organisation to send the e-mails in question. Accordingly, the Commission found that there was no breach of the Consent Obligation.

Case Summary

RE AIG ASIA PACIFIC INSURANCE PTE LTD

Consent Obligation *– Continued use of personal data for marketing purposes after appointed day*
Consent Obligation *– Withdrawal of consent*

25 February 2016

BACKGROUND

1 The Organisation is a general insurance company, which offers several products including motor insurance.

2 Sometime before the Personal Data Protection Act 2012[1] ("PDPA") came into full force on 2 July 2014 ("Appointed Day"), the Complainant bought a vehicle at a price that was packaged with an insurance cover and in-house financing provided by the Organisation. The Complainant had to fill up a Motor Insurance Proposal Form ("Form") for the insurance cover.

3 The Form contained sections for the Complainant to fill in his personal data, such as his mobile phone number and residential/mailing address. The Form, in a section captioned "Acknowledgement and Declaration", stated that the Organisation's collection of personal data was for, among other things, marketing purposes and ended with a declaration of consent ("Consent Clause").

4 Aside from the Consent Clause, the Form also contained information on how individuals could opt out of receiving marketing messages from the Organisation.

5 After signing up for the motor insurance cover, the Complainant started receiving marketing materials in his insurance policy pack from the Organisation by mail. In response, the Complainant sent an e-mail to the Organisation's customer care on 22 September 2014 ("22 September 2014 E-mail") wherein he stated that he did not opt to receive the marketing

1 Act 26 of 2012.

materials from the Organisation and asked why the Organisation was sending him such materials.

6 On 25 September 2014, the Complainant received a marketing phone call from the Organisation on his mobile phone number. During the call, the Complainant requested to opt out from receiving marketing calls. The request was effected immediately by the Organisation. Nevertheless, the Complainant proceeded to lodge a complaint with the Commission.

ISSUE

7 There are two issues arising in this case. The first issue is whether the Organisation was permitted under the PDPA to use the Complainant's personal data it had collected before the Appointed Day to send the marketing materials by mail to the Complainant.

8 The second issue is whether the Organisation was similarly permitted to make the marketing call on 25 September 2014, in view of the fact that the Complainant had allegedly withdrawn his consent[2] to use his personal data in his 22 September 2014 E-mail.

FINDINGS

9 In relation to the first issue, the Commission found that the Organisation was permitted to use the Complainant's personal data to send the marketing mail pursuant to s 19 of the PDPA. The Complainant's personal data was collected *before* the Appointed Day, and the use of his personal data for marketing purposes was consistent with the purposes for which his personal data was collected.

10 Even if the personal data was collected *after* the Appointed Day, the Organisation would still not be in breach of the PDPA as it had validly obtained consent from the Complainant to collect and use his personal data for the specified purposes of marketing through his acknowledgment of the Consent Clause in the Form.

11 In relation to the second issue, the Commission found that the 22 September 2014 E-mail was, at most, an indication by the Complainant

2 Pursuant to s 16 of the Personal Data Protection Act 2012 (Act 26 of 2012).

to the Organisation to stop using the Complainant's mailing address for marketing purposes. This did not extend to a request to stop using the Complainant's telephone number. It was not clear from the contents of the 22 September 2014 E-mail and the context in which that e-mail was sent that the Complainant had also intended for the Organisation to stop using his telephone number to send marketing messages.

12 Even if the Complainant's 22 September 2014 E-mail amounted to a withdrawal of consent, a reasonable time had to be allowed for the Organisation to put the withdrawal into effect. In the present case, the Commission took into consideration the fact that the call was made within three days of the Complainant's 22 September 2014 E-mail. Moreover, the Organisation had stated in its opt-out link that it aimed to comply with any opt-out request within 30 days of receipt. Accordingly, it was reasonable for the withdrawal to have not come into effect when the call was made on 25 September 2014.

13 The Commission found that the Organisation did not breach the PDPA by using the Complainant's personal data to mail and call him for marketing purposes.

Case Summary

RE PROPERTYGURU PTE LTD

Consent Obligation *– Obtaining consent – Pre-selected checkboxes*

11 March 2016

BACKGROUND

1 The Organisation provides a website that lists residential and commercial properties in Singapore for sale or rental. The Complainant received several marketing e-mails and text messages from the Organisation. Her complaint was that there was unauthorised use of her personal data by the Organisation in sending her the messages.

2 The Organisation obtained the Complainant's contact details through its website. Consent to send marketing messages was obtained through an "opt-in" process in the following manner. Each webpage listing a property also lists the property agent for that property. An interested user may fill in a form for the property agent to contact her. Just above the "contact agent" button of the form is a checkbox with the description: "Please send me updates, monthly newsletter and partner offers." By default, this checkbox is checked. Leaving the checkbox selected meant that the user would be deemed to have consented to receive marketing updates. To opt out of receiving such updates, the user had to un-check the checkbox. Investigations disclosed that the Complainant did not un-check the "opt-in" checkbox.

ISSUE

3 The issue is whether the Organisation had consent from the Complainant to collect and use the Complainant's e-mail address and

mobile phone number for the purposes of sending her the marketing messages, pursuant to the Consent Obligation.[1]

FINDINGS

4 In the Personal Data Protection Commission's view, the Organisation's website stated clearly that the contact details which the user provides would be used for marketing if the checkbox remains checked. The checkbox was located just above the "contact agent" button; it was displayed prominently and would have been hard to miss. In this regard, the Commission found that the Complainant's consent to receive marketing updates had been effectively obtained at the time she completed the online form. Since the Complainant did not withdraw her consent and the Organisation's use of her personal data was consistent with the purpose for which it had been collected, the Commission did not find the Organisation to be in breach of its Consent Obligation.

5 However, the Commission is of the view that it is not a good practice to use pre-selected checkboxes. There may be circumstances that may make it difficult for the organisation to subsequently demonstrate that it had obtained unambiguous consent from the individual, for example, where the checkboxes and descriptions are not sufficiently prominent. That said, the use of pre-selected checkboxes to obtain consent is not prohibited so long as the organisation is able to demonstrate that the purpose of collection, use and disclosure had been effectively notified at the time consent was obtained.[2]

---

1 Pursuant to ss 13 and 14 of the Personal Data Protection Act 2012 (Act 26 of 2012).

2 Specifically, s 14 of the Personal Data Protection Act 2012 (Act 26 of 2012).

Case Summary

RE OCEAN FRONT PTE LTD

Application of other written laws *– Building Maintenance and Strata Management Act (Cap 30C, 2008 Rev Ed)*
Consent Obligation *– Disclosure of personal data – Minutes of council meeting of Management Corporation Strata Title*

8 April 2016

BACKGROUND

1 The Complainants are owners and residents of a condominium. The Organisation is the managing body of the condominium (*ie*, the Management Corporation Strata Title ("MCST")). The complaint concerned the disclosure of personal data found in the minutes of the council meeting held by the MCST.

2 At the council meeting, the Complainants were the subjects of a complaint that they harassed, used vulgarities and made disparaging remarks at members of the MCST staff. The Complainants' names and apartment unit numbers were included in the MCST meeting minutes, which were posted outside the management office's notice board. The minutes were posted as a requirement of the Building Maintenance and Strata Management Act[1] ("BMSMA"). Shortly after such posting, the Complainants requested that the MCST remove the meeting minutes or remove the offending paragraphs within the meeting minutes from the version published on the notice board. The Organisation denied any wrongdoing but removed the Complainants' names and apartment unit numbers from the MCST meeting minutes. The Complainants alleged that the Organisation had disclosed their names and apartment unit numbers without their consent and notification.

1 Cap 30C, 2008 Rev Ed.

ISSUE

3 The key issue in this case is whether the MCST should have obtained the consent of the residents whose personal data would be disclosed in the MCST meeting minutes before posting the minutes on the MCST's notice board. Pursuant to s 13 of the Personal Data Protection Act 2012[2] ("PDPA"), organisations generally need consent to collect, use or disclose personal data about an individual unless an exception applies. One such exception is s 4(6) of the PDPA which generally provides for other laws to prevail over the PDPA where they are inconsistent.

FINDINGS

4 Under s 53(11) of the BMSMA read with para 3(2) of the Second Schedule to the BMSMA, the MCST is required to keep minutes of its proceedings and general meetings, display and keep a copy of any minutes on the MCST's notice board for not less than 14 days or give a copy of the minutes to each of the residents if there is no notice board. The relevant BMSMA provisions appeared to allow the entire meeting minutes to be disclosed without redaction of any personal data contained therein. Pursuant to s 4(6) of the PDPA, the BMSMA provisions take precedence over the consent requirements under the PDPA. Therefore, the MCST could post the entire meeting minutes containing personal data without obtaining consent. In any case, since the Organisation had already removed the Complainants' names and apartment unit numbers from the meeting minutes at the Complainants' request, the Personal Data Protection Commission did not take any further action in the matter.

---

2 Act 26 of 2012.

Case Summary

RE BLACK PEONY

Consent Obligation *– Disclosure of personal data – Whether disclosure on social media was for purposes that a reasonable person would consider appropriate in the circumstances*
Personal data *– WhatsApp chats not personal data* per se

11 April 2016

BACKGROUND

1 The Organisation provides beauty and spa services and the Complainant was one of its customers. The Complainant alleged that the Organisation had disclosed her personal data on the Internet without her consent in breach of the Personal Data Protection Act 2012[1] ("PDPA").

2 The complaint arose out of a disagreement over the services received by the Complainant. The Complainant was dissatisfied with the Organisation's service and posted a negative review detailing her unsatisfactory service experience on the Organisation's Facebook page as well as on an online forum. The Complainant's name, photograph and username on the online forum were disclosed in her reviews.

3 The Organisation responded to the negative reviews in a blog post that referred to the Complainant's negative reviews and posted screenshots of WhatsApp messages and chats between the Complainant and the Organisation. A copy of the police report lodged by the Organisation against the Complainant, which contained the Complainant's name, age and occupation, was also published in the blog post.

4 The Organisation also posted on an online forum, setting out the Complainant's allegations against the Organisation, which included the Complainant's name and username on another online forum, as well as the Organisation's response.

1 Act 26 of 2012.

ISSUE

5 The main issue in this case is whether the Organisation complied with its Consent Obligation[2] in respect of the disclosure of the Complainant's personal data online.

FINDINGS

6 From the Personal Data Protection Commission's investigations, most of the personal data that the Organisation had disclosed was already made available online by the Complainant. These included the Complainant's name; the same photograph of the Complainant as the one the Organisation posted; and her username. What the Organisation had disclosed on the blog and forum, and which the Complainant had not previously disclosed, were the private communications between the Complainant and the Organisation (*ie*, the WhatsApp messages, *etc*). Private communications such as WhatsApp messages and chats are not necessarily personal data in and of themselves.

7 In the Commission's view, where an individual chooses to engage an organisation publicly, there can be circumstances where the use or disclosure of personal data may be made without consent if it would be reasonable to do so. This may include situations where an individual makes an allegation or complaint against the organisation publicly but it is reasonable to expect that consent for the organisation to use the individual's personal data to respond to the allegations would not be forthcoming.

8 Although it may be reasonable for the organisation to use and disclose personal data without consent or notification in certain situations, the Commission would emphasise that in line with the standard of reasonableness that underpins the PDPA,[3] any such use or disclosure of personal data should be proportionate and be limited to what is reasonable for the organisation to respond to the individual's allegations and complaints.

---

2 Pursuant to s 13 of the Personal Data Protection Act 2012 (Act 26 of 2012).

3 As provided for in s 11 of the Personal Data Protection Act 2012 (Act 26 of 2012).

9 In this case, the Complainant chose to post her comments and engage the Organisation over the unsatisfactory service she received from the Organisation in publicly accessible posts online. Based on the Organisation's response on the blog and forum, there was nothing to show that the Organisation had been excessive or unreasonable in the use or disclosure of the Complainant's personal data.

10 This was an ongoing dispute that the Complainant had chosen to air on publicly accessible fora: *ie*, the Organisation's Facebook page as well as on an online forum. After the Organisation's public defence of the allegations made against it, the Complainant brought the dispute to the Commission. In these circumstances, the Commission decided not to take any further action in the matter as the complaint was not made in good faith.

Case Summary

RE MYTUITIONCLUB PTE LTD

Business contact information *– Tutor's contact details*
Consent Obligation *– Disclosure of personal data without consent – Whether business contact information exemption applied*

13 April 2016

BACKGROUND

1 The Organisation is a company which provides services to match tutors with students. The Complainant had enrolled herself as a private tutor with the Organisation. The Complainant and the Organisation entered into an agreement for the Organisation's services.

2 In the course of providing tuition services, the Complainant failed to fulfil a tuition assignment. The Organisation contended that the Complainant had breached the agreement with the Organisation, and sought to claim from the Complainant a penalty fee of $135.

3 The Organisation warned the Complainant that the failure to pay the penalty fee would entail the Complainant being blacklisted on the Organisation's website. An additional fee of $100 would also be levied on the Complainant should she wish to remove her name from the blacklist.

4 The Complainant gave the Organisation an explanation for her failure to fulfil the tuition assignment, but the Organisation rejected her explanation. After several reminders for payment, the Organisation proceeded to publish the Complainant's full name, e-mail address, contact number and a partially-masked National Registration Identity Card ("NRIC") number on the Organisation's website blacklist. Only the last two numerical digits of the NRIC number were masked. There was also a brief description of what the Organisation claimed to be the Complainant's infraction of their agreement.

ISSUE

5 Under the Personal Data Protection Act 2012[1] ("PDPA"), an organisation would need to obtain consent before disclosing personal data, unless an exception applies.[2] No such consent was obtained before the Organisation had published the Complainant's particulars on its website. However, there is an exception to consent where the personal data is business contact information ("BCI").[3] If the Complainant's personal data was BCI, the Organisation would not need to obtain the Complainant's consent to disclose the information on the Organisation's website.

FINDINGS

6 When contact details are provided for the purposes of carrying on business, the contact details would be considered BCI. In the present case, the provision of tuition services is a form of business. Accordingly, the contact details provided by the tutor to facilitate communications with her in the course of providing tuition services are BCI.

7 On the facts of this case, it was not entirely clear that the Complainant's information was provided as BCI. The agreement between the Organisation and Complainant was a standard form that had a field for the Complainant's next-of-kin contact details, suggesting that not all fields were provided as BCI. Additionally, the information provided appeared to be subject to the confidentiality clause in the form. This suggests that some of the information was not meant to be used for wider dissemination.

8 Given the contraindications to the general premise that a person's particulars provided for carrying on business are BCI, the Personal Data Protection Commission was of the view that it would be unsafe to make a finding on the issue in the absence of clear evidence one way or the other. While the NRIC number was probably not BCI, it was a masked version that was posted on the black list. Apart from this, the BCI exception probably applied to the rest of the Complainant's contact details that were posted on the black list. As such, it could not be clearly established that the

---

1 Act 26 of 2012.

2 Pursuant to ss 13 and 14 of the Personal Data Protection Act 2012 (Act 26 of 2012).

3 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(5).

Organisation had breached the PDPA. Accordingly, the Commission decided not to proceed further with the matter and issued an advisory notice to the Organisation.

Case Summary

RE CBRE PTE LTD

Protection Obligation *– Disposal of personal data – Administrative and physical security arrangements*

12 May 2016

BACKGROUND

1 A journalist informed the Personal Data Protection Commission that she had retrieved documents containing personal data from the garbage area of an office building. Among the documents retrieved which concerned the Organisation, a real estate agency, were two documents, namely a letter of intent in respect of a lease of a property in Singapore and a fee advice in respect of another property. Both the letter of intent and the fee advice contained personal data of individuals involved in the transactions, such as the landlord and occupant's names and identification numbers as well as the agents' names and fees.

ISSUE

2 The key issue is whether the Organisation had made reasonable security arrangements and satisfied its Protection Obligation.[1]

FINDINGS

3 The Organisation had in place policies that dealt with the Organisation's data protection obligations, including business records retention and destruction/disposal policies, policies which dealt with the use and disclosure of confidential information, information security protocols as well as security measures for physical documents and electronic documents. The Organisation also conducted regular training for its employees and set out specific guidance on disposing of confidential and

1 Pursuant to s 24 of the Personal Data Protection Act 2012 (Act 26 of 2012).

proprietary information as well as its policies in relation to information security in its Code of Conduct and Employment Handbook.

4 While the Organisation had these policies and practices in place, it was apparent that in the present case, these policies and practices were not followed by the Organisation's staff to ensure the proper disposal of the documents. However, there was no indication that this was a systemic or recurrent issue within the Organisation. The Organisation was found to have put in place reasonable policies and practices.

5 The Organisation would have discharged its Protection Obligations under the Personal Data Protection Act 2012[2] if it conducted itself in a manner that a reasonable person would consider appropriate in the circumstances.[3] In the final analysis, the Commission decided that the Organisation had conducted its affairs reasonably and appropriately. Therefore, the Commission found that there was no breach in this case.

---

2 Act 26 of 2012.

3 Pursuant to s 11(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

Case Summary

RE INTERFLOUR GROUP PTE LTD

Consent Obligation *– Collection of personal data – Inadvertent access to former employee's personal e-mails*
Personal data *– E-mails not personal data* per se

21 July 2016

BACKGROUND

1 The Complainant, a former employee of the Organisation, alleged that the Organisation had accessed his personal e-mail account ("Hotmail account") without his consent after he left the employment of the Organisation. The unauthorised access only ceased when the Complainant changed the password to his Hotmail account.

2 It was the Organisation's usual practice to continue accessing the Complainant's work laptop to retrieve documents and information on the projects that the Complainant had been working on after his employment ended. However, unknown to the Organisation at the time, the Complainant had configured the e-mail program on his work laptop to automatically log into and download e-mails from his personal Hotmail account without prompting for a password whenever it was started. Hence, whenever the Organisation accessed the Complainant's Outlook e-mail program to check his work e-mails, it would also inadvertently access his personal Hotmail account. The e-mails from the Complainant's work e-mail account and personal Hotmail account would be intermingled and displayed in a universal Inbox.

3 The Organisation admitted accessing the Complainant's Hotmail account in this manner but denied that such access was unauthorised access because the Complainant had configured his office e-mail program on his work office laptop to automatically log into his personal Hotmail account.

ISSUE

4 The issue in this case is whether the Organisation was in breach of its Consent Obligation by accessing the Complainant's Hotmail account.[1]

FINDINGS

5 The Personal Data Protection Commission limited its assessment to aspects relating to personal data protection law. Here, there was no evidence which suggests that the Organisation had gained access to the e-mails from the Complainant's Hotmail account by any means other than through the auto-login function which was configured by the Complainant himself. It therefore appeared that access to these e-mails was inadvertent.

6 The Complainant's personal data involved in this case are (a) his username and password to his Hotmail account and (b) such of his personal data stored in the account (for instance, in the content of e-mail messages). The Complainant had supplied and stored his username and password to his Hotmail account when he set the Outlook e-mail program to automatically log into and access his personal e-mails. The username and password were stored by him directly in the Outlook e-mail program. As the Organisation was not aware of the Complainant's actions, it cannot be said that the Organisation had *collected* this set of personal data. However, the situation would be different once the Organisation knows that the username and password had been stored in the Outlook e-mail program and continues to *use* it to access the Complainant's personal Hotmail account. The pertinent questions are whether there is consent to use this personal data; whether there was effective withdrawal of consent; and whether any of the exceptions to consent are applicable to permit continued use without consent.

1 Pursuant to ss 13 to 17 of the Personal Data Protection Act 2012 (Act 26 of 2012).

7 The question of consent requires an analysis of the Organisation's policies relating to the use of personal e-mail accounts on notebooks and other computing devices that it issues as well as whether the Complainant had a practice of using his personal e-mail account for work-related communications. This inquiry may lead to the conclusion that there may be express or deemed consent. The question whether consent was effectively withdrawn requires an examination of the conduct of the Complainant and his communications with the Organisation. Finally, whether the Organisation may rely on one of the exceptions to consent in the Third Schedule to the Personal Data Protection Act 2012[2] ("PDPA") depends on the circumstances of any continued use: *eg*, the Organisation may seek to rely on the investigation or proceedings exception if it was investigating an alleged breach by the Complainant of his terms of employment or duty of fidelity to the Organisation.

8 Next, while an e-mail message may contain personal data, e-mail messages are not personal data *per se*. An e-mail message has to contain information about an individual before it may be said to constitute personal data within the meaning of the PDPA. By setting up his personal Hotmail account in Microsoft Outlook, the Complainant had voluntarily provided the Organisation with his personal Hotmail e-mail address and other personal information stored in the Hotmail profile within Microsoft Outlook. E-mails that are downloaded from Hotmail will contain the Complainant's Hotmail e-mail address and Microsoft Outlook will display other personal information stored in the Hotmail profile, *eg*, his name or nickname. Apart from these, there was insufficient evidence that e-mail messages downloaded from the Complainant's Hotmail account contained any other of his personal information.[3]

9 In the course of investigations, the Commission was informed that the Complainant had lodged a complaint with the police alleging Computer Misuse and Cybersecurity Act[4] offences against the Organisation; and that

2 Act 26 of 2012.

3 As the question of whether the Organisation collected personal data of persons other than the Complainant (for instance, persons sending e-mails to him or persons to whom he sent e-mails) was not the subject matter of the complaint, the Personal Data Protection Commission made no findings in respect of these issues.

4 Cap50A, 2007 Rev Ed.

there are ongoing civil claims between the Complainant and the Organisation on breach of confidentiality and unpaid salary. In view of the pending police investigations and civil claims, the Commission discontinued investigations into the matter and issued an advisory notice to the Organisation.

Case Summary

RE NATURALLY PLUS SINGAPORE PTE LIMITED

Purpose Limitation Obligation *– Whether collection, use and disclosure of personal data were for purposes that a reasonable person would consider appropriate in the circumstances*
Retention Limitation Obligation *– Retention of verification documents for one year*

28 March 2017

BACKGROUND

1 This case arose from a complaint about the Organisation's alleged over-collection of personal data during the purchase of the Organisation's products.

2 Specifically, when a member purchases a product using a third party's credit card without the member and credit card holder being physically present at the Organisation's premises, the member would be required to furnish photocopies of the front of the credit card and the credit card holder's National Registration Identity Card or Work Permit ("Required Documents"). This requirement was instituted around mid-2016 pursuant to a directive from the Organisation's merchant agent ("Agent"), which provided credit card point of sale terminals and gateway services to the Organisation. The Agent's directive was in response to a fraud case involving the Organisation in early-2016.

3 The Organisation used the Required Documents to perform verification matching of the personal data to ensure consistency and authenticity of the third-party credit card holder. The credit card holder would be contacted if inconsistencies were detected. In the event of a potential fraud investigation, the Organisation would also release the Required Documents to its Agent.

4 The Organisation had internal data protection policies in place and stored the Required Documents in its internal warehouse under secured conditions with access limited to only authorised personnel.

5 The Organisation also instituted a one-year retention period for the Required Documents, on the basis that this would be sufficient to resolve any possible credit card fraud.

ISSUES

6 Two issues arose in this case. The first issue is whether the Organisation's collection, use and disclosure of personal data in the Required Documents was for purposes that a reasonable person would consider appropriate in the circumstances, pursuant to the Purpose Limitation Obligation.[1]

7 The second issue is whether the Organisation's retention period of one year for the Required Documents was in compliance with the Retention Limitation Obligation.[2]

FINDINGS

8 In respect of the Purpose Limitation Obligation, the Personal Data Protection Commission observed that the Organisation's purpose for collecting the Required Documents was to ensure the authenticity of the transaction to prevent potential fraud. The Organisation's verification process served to provide reasonable assurance to the Agent and the Organisation's members of its anti-fraud measures, protected the Organisation's business interest in credit card fraud prevention and reduced its potential liability in the event of a fraud.

9 The Commission deliberated whether there were other alternatives to the Required Documents, given the sensitivity of the personal data involved. The Commission concluded that, unlike the NRIC/Work Permit, other forms of identification may not have the requisite provenance or contain the particulars required for the Organisation's verification purposes and may not be applicable to all members. The Commission further observed that the Organisation has minimised the personal data collected by requiring only photocopies of the front of the Required Documents.

---

1 Pursuant to s 18 of the Personal Data Protection Act 2012 (Act 26 of 2012).

2 Pursuant to s 25 of the Personal Data Protection Act 2012 (Act 26 of 2012).

10 As for the Retention Limitation Obligation, the Commission observed that whilst the Organisation's general retention period is five to seven years for company documents for accounting and tax purposes, the Organisation had instituted a retention period of only one year for the Required Documents and took practical steps to limit the retention of the Required Documents.

11 The Commission was satisfied that the Organisation had adequately discharged the Purpose Limitation Obligation and Retention Limitation Obligation.

12 Notwithstanding the decision to find the Organisation not in breach in this instance, the Commission emphasises that excessive collection of personal data poses data protection risks and liabilities to organisations. Organisations are strongly advised to restrict their collection of personal data from customers to legitimate business purposes, failing which they could be found to have contravened the Purpose Limitation Obligation under the Personal Data Protection Act 2012.[3]

---

3 Act 26 of 2012.

Case Summary: Review Application

RE THE FULLERTON HOTEL

Access Obligation *– Whether Applicant was entitled to request access to view closed-circuit television footage – Personal data no longer existed*

18 December 2014

BACKGROUND

1 The Applicant brought an application for review under s 28(1) of the Personal Data Protection Act 2012[1] ("PDPA") alleging that the Organisation had refused to provide access to closed-circuit television ("CCTV") footage containing his personal data.

2 The Applicant requested access to CCTV footage of an alleged fight that took place outside one of the Organisation's premises. Access was denied because the Organisation's policy was that CCTV footage was for their own use and would not be disclosed unless it was in connection with any investigation conducted by a government authority. In any case, the Organisation claimed that it had reviewed the CCTV footage recorded on the relevant date and location based on the information provided by the Applicant but was unable to find any identifiable images of the Applicant. A representative of the Organisation had also affirmed a statutory declaration confirming that by the time the Applicant brought its application for review, the CCTV footage of the relevant day no longer existed as the footage had already been overwritten with new footage.

ISSUE

3 The issue is whether the Applicant is entitled to his request for access to the personal data contained in the Organisation's CCTV footage pursuant to s 21 of the PDPA.

1 Act 26 of 2012.

FINDINGS

4 The right to make a request for access is not limited to cases where the individual has made a police report. Therefore, it was incorrect for the Organisation to take the position that an individual was only entitled to access to the individual's personal data when an investigation was conducted by a government authority.

5 In this case, the Organisation was required to review its CCTV footage for identifiable images requested by the Applicant and provide access to the images. Even if the CCTV footage had contained identifiable images of other individuals, pursuant to s 21(5) of the PDPA and to the extent that it was possible to do so, the Organisation would have been required to mask the images of other individuals and to provide the individual access to the edited CCTV footage. However, given that the CCTV footage requested had ceased to exist at the time of the application, the Organisation was not required to provide the CCTV footage pursuant to para 1(*j*)(iii) of the Fifth Schedule to the PDPA.

6 The Personal Data Protection Commission highlights that organisations should, as soon as reasonably possible after receiving an access request, ensure that the personal data requested is preserved in order to meet its obligation under s 21(1) of the PDPA. This may extend to such time until the Commission has concluded its review of the access request and any right of the individual to apply for reconsideration and appeal is exhausted.

Case Summary: Review Application

RE RSH KIDS PTE LTD

Access Obligation *– Whether Applicant was entitled to request access to view closed-circuit television footage – Personal data no longer existed*

22 January 2016

BACKGROUND

1 The Applicant brought a review application pursuant to s 28(1) of the Personal Data Protection Act 2012[1] ("PDPA") against the Organisation's refusal to provide access to his two-year-old son's personal data in accordance with s 21(1) of the PDPA. The Applicant's child was enrolled in the Organisation's kindergarten and sustained an injury from a fall on the Organisation's premises. The incident was investigated by both the sector regulator, the Early Childhood Development Agency ("ECDA"), as well as the police.

2 After the incident, the Applicant requested for access to closed-circuit television ("CCTV") footage of his child's fall within the Organisation's premises but the Organisation rejected the Applicant's request on the grounds that the CCTV footage was purely for the Organisation's internal use and was not open to any request for access unless legal action was required by enforcement agencies such as the police or the ECDA.

3 The Organisation's CCTV system could only record and store a maximum of seven days' worth of video footage, after which the footage recorded earlier would be overwritten. The Organisation claimed that it did not know how to access its CCTV system to download a copy of the CCTV footage but the Organisation's employee had used his mobile phone to make a video recording of the CCTV footage as it was played. As such, when the ECDA and police officers visited the Organisation's premises to investigate the incident, they were able to view the copy of the CCTV footage of the incident on the employee's mobile phone. However, by the

1 Act 26 of 2012.

time the Applicant filed a review application with the Personal Data Protection Commission, the CCTV footage had already been overwritten and the employee had deleted the video recording of the CCTV footage from his phone as the investigations by the ECDA and the police had been completed. Therefore, the personal data requested by the Applicant no longer existed in the possession or under the control of the Organisation.

ISSUE

4 The issue is whether the Applicant is entitled to his request for access to the personal data contained in the Organisation's CCTV footage pursuant to s 21 of the PDPA.

FINDINGS

5 The PDPA does not limit the obligation to provide access to personal data to only those specific situations where legal enforcement is required by law enforcement agencies. The data subject's access rights are independent of any legal enforcement action.

6 The Commission highlights that law enforcement agencies have far reaching investigatory powers that they can exercise in order to obtain CCTV footages that are necessary for their investigations and would not need to rely on the data subject exercising his access rights in order to obtain copies for the purpose of investigations.

7 Organisations are prohibited from providing access to the requested personal data if such provision would reveal the personal data of other individuals;[2] this prohibition does not apply if it is possible for the Organisation to exclude the personal data of those other individuals from the copy of the CCTV footage that is provided. This includes masking images of other individuals captured in the CCTV footage.

8 However, in view of the fact that the personal data requested no longer existed in the Organisation's possession or control, the Organisation cannot be directed to provide access to the personal data requested in this case pursuant to para 1(*j*)(iii) of the Fifth Schedule to the PDPA. An

2 Section 21(3) read with s 21(5) of the Personal Data Protection Act 2012 (Act 26 of 2012).

advisory notice was issued to the Organisation to remind it of its obligations under the PDPA in this matter.

9 The Commission highlights that organisations should, as soon as reasonably possible after receiving an access request, ensure that the personal data requested is preserved in order to meet its obligation under s 21(1) of the PDPA. This may extend to such time until the Commission has concluded its review of the access request and any right of the individual to apply for reconsideration and appeal is exhausted.

Case Summary: Review Application

RE MANAGEMENT CORPORATION STRATA TITLE PLAN NO 2956

Access Obligation *– Whether Applicant was entitled to request access to closed-circuit television footage – Personal data no longer existed*
Openness Obligation *– Inadequate data protection policies and practices*

5 September 2016

BACKGROUND

1 The Organisation is a managing body of a private housing compound; the Applicant is a resident of the housing compound. The Applicant wrote an e-mail to the Organisation requesting access to his personal data contained in the form of closed-circuit television ("CCTV") footage. The CCTV footage in question allegedly recorded a dispute between the Applicant and another individual that occurred in the car park lift lobby of the housing compound. The Organisation did not respond to the Applicant's request.

2 The Applicant then lodged a review application with the Commission against the Organisation in respect of the alleged failure of the Organisation to provide him access to his personal data pursuant to s 21(1) of the Personal Data Protection Act 2012[1] ("PDPA"), and requested that the Organisation be directed to provide him access to the CCTV footage.

3 In its written response to the review application, the Organisation submitted an explanation of its refusal to provide access to the personal data requested by the Applicant. The Organisation also confirmed that the requested CCTV footage containing the Applicant's personal data had already been deleted.

1 Act 26 of 2012.

ISSUE

4 The issue is whether the Commission ought to grant the direction for access to the CCTV footage under s 28 of the PDPA, as requested by the Applicant.

FINDINGS

5 Based on the information provided by the Organisation, the CCTV footage was no longer in the possession or under the control of the Organisation as it was the Organisation's practice to only retain the CCTV footage for up to two weeks. Given that the alleged dispute took place 17 weeks before the Applicant made his access request to the Organisation, the relevant CCTV footage would have been deleted by the time the Applicant made his access request.

6 In the circumstances, the Organisation cannot be directed to provide the Applicant access to the CCTV footage containing his personal data as the CCTV footage would have been already deleted. Not only would it be impossible for the Organisation to give effect to the direction sought by the Applicant, such a direction would also serve no practical purpose.

7 Notwithstanding that the CCTV footage had already been deleted, the Organisation should have responded in a timely manner to the Applicant's request. With regard to its lack of a timely response, the Organisation claimed that there were insufficient details provided by the Applicant in his access request. However, this is not a valid or recognised exception under the Fifth Schedule to the PDPA and therefore does not exempt the Organisation from its obligations under s 21(1) of the PDPA. The Organisation ought to have engaged the Applicant in order to seek clarification of the details of his request, and if the CCTV footage was deleted, the Organisation could have communicated this fact to the Applicant.

8 Likewise, the Organisation's claims that only one request was made and no repeated requests were submitted; that there was no "police order" made; and that the Applicant had a record of "creating nuisance" to the Organisation, are not valid or recognised exceptions under the Fifth Schedule to the PDPA. The Organisation is therefore not exempt from its obligation under s 21 of the PDPA by these claims.

9 In addition, investigations also found that the Organisation did not develop and implement policies that are necessary for it to meet its obligations under the PDPA, communicate these policies and practices to its staff, and make these policies and practices available upon request, pursuant to s 12 of the PDPA.

10 In consideration of the above, the Personal Data Protection Commission issued the Organisation with an advisory notice to remind it of its data protection obligations, specifically the Openness and Access Obligations under ss 12 and 21 of the PDPA respectively.

DEVELOPMENT OF SINGAPORE DATA PROTECTION LAW: INTERNATIONAL INFLUENCES AND LOCAL NEEDS*

David N ALFRED†
LLB, LLM (Intellectual Property and Technology Law) (National University of Singapore), MBA (Chicago); Advocate and Solicitor (Singapore), Solicitor (England & Wales); CIPP/A

1 Data protection law[1] is a relatively modern branch of law internationally, with laws first appearing in a few jurisdictions in the 1970s and several countries later enacting laws based on the principles of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* which was published by the Organisation for Economic Co-operation and Development ("OECD") in 1980 ("OECD Guidelines").[2] One notable development during this period was the European Union's Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("EU Directive").[3] The EU Directive sought to harmonise the data protection laws of EU Member States but its influence extended to other

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors remain the author's own.

† Chief Counsel, Personal Data Protection Commission.

1 Data protection law is also referred to as data privacy law or information privacy law. Such laws generally concern the protection of information about an identifiable individual, which may be referred to as personal data, personal information or personally identifiable information (although the scope of protection may vary across different laws).

2 The first modern data protection law was introduced in the German state of Hesse in 1970.

3 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 (hereinafter "EU Directive"). The EU Directive built on earlier European instruments including the European Convention on Human Rights (see Art 8.1 on the right to respect for private and family life) and the Council of Europe's Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (ETS No 108).

countries as a result of its requirements concerning transfer of personal data to countries outside the EU (amongst other reasons).

2 Significant developments in information and communications technology ("ICT") since 2000 have led to a renewed interest in this area of law and several more countries have enacted data protection laws since mid-2000.[4] Some countries which had earlier enacted data protection laws have also reviewed and enhanced their laws in recent years.[5] The Asia-Pacific Economic Cooperation forum ("APEC") published the *APEC Privacy Framework* ("APEC Framework") in 2005, and a revised edition of the OECD Guidelines, the *OECD Privacy Framework*, was published in 2013 ("OECD Framework"). Singapore was one of the countries to enact a law in this later phase, the Personal Data Protection Act 2012[6] ("PDPA"). The PDPA was the first general data protection law in Singapore.[7] Its provisions relating to the establishment of Singapore's data protection authority, the Personal Data Protection Commission ("PDPC"), came into

4 For example, see India's Information Technology Act (No 21 of 2000) (amended in 2008 to include provisions relating to the processing of sensitive personal data), Malaysia's Personal Data Protection Act 2010 (Act 709), the Philippines' Data Privacy Act of 2012 (Republic Act No 10173) and South Korea's Personal Information Protection Act (Act No 10465) (enacted in 2011). Indonesia and Thailand may pass similar laws in the future.

5 For example, see Australia's Privacy Act 1988 (No 119) (enacted in 1988 and last amended in 2014 to strengthen the powers of Australia's Privacy Commissioner), Japan's Act on the Protection of Personal Information (Act No 57 of 2003) (enacted in 2003 and amended in 2016 with provisions establishing Japan's Personal Information Protection Commission) and Hong Kong's Personal Data (Privacy) Ordinance (ER 1 of 2013) (Cap 486) (enacted in 1995 and amended in 2013 to include provisions on use of personal data in direct marketing).

6 Act 26 of 2012.

7 Prior to the enactment of the Personal Data Protection Act 2012 (Act 26 of 2012), some sectoral regimes in Singapore provided a degree of protection for personal data. See, for example, s 47 of the Banking Act (Cap 19, 2008 Rev Ed) (on the protection of banking customers' information), s 25 of the Infectious Diseases Act (Cap 137, 2003 Rev Ed) (on the protection of the identity of individuals with AIDS and certain other diseases) and para 3.2.6 of the Telecom Competition Code 2005 (S 87/2005) (on unauthorised use of telecom subscribers' information).

force on 2 January 2013[8] while its provisions relating to the protection of personal data[9] ("Data Protection Provisions") came into force on 2 July 2014.[10]

3 This article considers the background to the enactment of the PDPA and the international influences and sources affecting its development.

I. Early approach – The Model Code

4 The impact of the EU Directive in Singapore was studied by the National Internet Advisory Committee ("NIAC").[11] In 2002, the NIAC issued a *Model Data Protection Code for the Private Sector* ("Model Code") together with a report of its Legal Subcommittee ("NIAC Report").[12] The Model Code was based on the principles of the OECD Guidelines and was modelled after the Canadian Standards Association's *Model Code for the Protection of Personal Information* ("CSA Model Code"). As Singapore did not have a general data protection law at that time, the Model Code provided a voluntary mechanism for organisations in the private sector to implement and abide by a set of data protection principles that was aligned with recognised international standards.

---

8 Singapore's Info-communications Media Development Authority has been designated as the Personal Data Protection Commission with effect from 1 October 2016 and a Commissioner for Personal Data Protection has been appointed to administer and enforce the Personal Data Protection Act 2012 (Act 26 of 2012) (see ss 5(1), 8(1) and 8(2)).

9 These include Pts III–VI and the Second to Sixth Schedules to the Personal Data Protection Act 2012 (Act 26 of 2012).

10 In addition, the "Do Not Call" provisions of the Personal Data Protection Act 2012 (Act 26 of 2012) (which regulate certain telemarketing activities) came into force on 2 January 2014.

11 The National Internet Advisory Committee was appointed by the (then) Ministry of Information and the Arts to advise on various aspects of the Internet.

12 National Internet Advisory Committee Legal Subcommittee, *Report on a Model Data Protection Code for the Private Sector* <unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012665.pdf> (accessed 15 May 2017) (hereinafter "NIAC Report").

5 The NIAC Report stated that the aim of the Model Code was to "strike a balance, in this information age, between the legitimate information needs of businesses, industries and institutions, on the one hand, and individuals' interests in the protection of their personal data, on the other".[13]

6 The NIAC Report noted two key developments which prompted the development of the Model Code. They were, first, developments in ICT which gave rise to new challenges in governing cyberspace and, secondly, the significance of the EU Directive to Singapore, particularly with respect to the free flow of data between countries. The NIAC Report summarised the first development succinctly:[14]

> With the advent of the information age comes the potential for mischief on an unprecedented level, both in terms of nature and scale. Data protection regimes impose discipline over a new breed of technology practitioners, who are yet to be regulated by any code of ethical behaviour, but who wield tremendous power over consumers by virtue of their potential to control personal data. Such discipline bolsters the confidence of consumers in the integrity of the e-commerce (and m-commerce) market, thus encouraging the increased automation of transactions between businesses and their customers, as Singapore strives to become an info-communications hub in a fully networked world.

7 On the second development, the NIAC Report highlighted two areas where the EU Directive may affect Singapore:

> (a) Art 25 of the EU Directive prohibited EU Member States from transferring personal data to countries outside the EU (third countries) which do not ensure an adequate level of protection for such data; and
>
> (b) the EU Directive may also require third countries which receive personal data from an EU Member State to have restrictions in place against the onward transfer of such data to other countries which do not ensure an adequate level of protection for such data.[15]

8 The NIAC Report concluded that there was thus the possibility of the flow of data from EU Member States to Singapore (whether directly or

13 NIAC Report at para 1.2.

14 NIAC Report, Executive Summary at para 3.1.

15 NIAC Report, Executive Summary at para 2.1.

through third countries) being impeded and this could, in turn, impede international trade and place Singapore businesses at a disadvantage in the global economy.[16]

9 The Model Code was subsequently adopted by the National Trust Council for its TrustSg programme and voluntarily implemented by various local businesses.

II. Development of the Personal Data Protection Act

A. Main themes leading to the development of the Personal Data Protection Act

10 In September 2011, Singapore's Ministry of Information, Communications and the Arts ("MICA") issued a public consultation on a proposed consumer data protection regime for Singapore ("First Consultation"). Two subsequent public consultations were held, in October 2011 and March 2012, on the framework for the establishment of a national "Do Not Call" ("DNC") registry ("Second Consultation") and the proposed Personal Data Protection Bill ("Third Consultation").

11 In its consultation paper for the First Consultation,[17] MICA addressed developments in the business and technological landscape which necessitated a stronger data protection regime, as well as the importance of cross-border data transfers to the Singapore economy. On the first issue, MICA noted that personal data had become increasingly valuable for

16 NIAC Report, Executive Summary at paras 2.2 and 2.3. The NIAC Report also indicated that some third countries had indeed enacted data protection laws which include restrictions against the transfer of personal data to countries which did not provide an adequate level of protection for personal data.

17 *Consultation Paper on a Proposed Consumer Data Protection Regime for Singapore* (Ministry of Information, Communications and the Arts, 13 September 2011).

businesses and more easily collected and processed with ICT[18] and explained:[19]

> There is an increasing need to protect consumers' personal data, especially in an era where personal data is becoming more and more valuable to businesses. There is a growing concern that consumers' personal data is being sold or used without their consent. This is exacerbated by new technologies that create new potential for infringements of consumer privacy even as they develop new opportunities to improve everyday life. Moreover, with technology becoming more unobtrusive, intelligent and pervasive, individuals have less control over the collection and use of their personally identifying data.

12 MICA also noted that the current regime placed the burden disproportionately on individuals to ensure that their personal data were protected and to pursue any suspected misuse "after the damage has already been done". Further, the voluntary approach of the Model Code meant that some organisations could choose not to abide by its requirements and this could undermine consumers' trust in the industry in general.[20]

13 Concerning cross-border transfers, MICA emphasised the importance of having a data protection law in relation to Singapore's role as a trusted hub for global data management and data processing activities.[21] MICA also noted that a lack of such legislation could have a broader impact on the flow of information between Singapore and other countries and place

18 *Consultation Paper on a Proposed Consumer Data Protection Regime for Singapore* (Ministry of Information, Communications and the Arts, 13 September 2011) at para 1.3.

19 *Consultation Paper on a Proposed Consumer Data Protection Regime for Singapore* (Ministry of Information, Communications and the Arts, 13 September 2011) at para 2.6.

20 *Consultation Paper on a Proposed Consumer Data Protection Regime for Singapore* (Ministry of Information, Communications and the Arts, 13 September 2011) at para 2.7.

21 *Consultation Paper on a Proposed Consumer Data Protection Regime for Singapore* (Ministry of Information, Communications and the Arts, 13 September 2011) at para 2.9.

Singapore businesses at a disadvantage in the global economy. The consultation paper concluded on this issue by stating:[22]

> [Data protection] legislation is increasingly seen as a basic feature in the legal framework for most economies. Sophisticated clients expect their personal data to be properly safeguarded regardless of geographical location. Having a general [data protection] legislation in place may thus facilitate the cross-border flow of information and facilitate the growth of Singapore businesses.

14 In light of these issues, MICA identified the following two key objectives for its proposed consumer data protection regime:[23]

a. To ensure there are adequate safeguards to protect consumers' personal data and promote greater consumer trust in the private sector; and
b. To strengthen Singapore's overall economic competitiveness and enhance Singapore's status as a trusted hub and choice location for global data management and processing services.

15 These points were also noted in Parliament during the second reading speech of the Personal Data Protection Bill[24] by the Minister for Information, Communications and the Arts (as he then was), Assoc Prof Dr Yaacob Ibrahim, who stated:[25]

> The personal data protection law will safeguard individuals' personal data against misuse by regulating the proper management of personal data. Individuals will be informed of the purposes for which organisations are collecting, using or disclosing their personal data, giving individuals more control over how their personal data is used. A data protection law will also enhance Singapore's competitiveness and strengthen our position as a trusted business hub. It will put Singapore on par with the growing list of countries that have enacted data protection laws and facilitate cross-border transfers of data.

---

22 *Consultation Paper on a Proposed Consumer Data Protection Regime for Singapore* (Ministry of Information, Communications and the Arts, 13 September 2011) at para 2.10.

23 *Consultation Paper on a Proposed Consumer Data Protection Regime for Singapore* (Ministry of Information, Communications and the Arts, 13 September 2011) at para 3.1.

24 Bill No 24 of 2012.

25 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

16 The importance of having a data protection regime which facilitates and enables cross-border transfers of data is well recognised internationally. The Foreword to the APEC Framework highlights the benefits to consumers, businesses and governments from economic and developmental perspectives. It states:

> APEC member economies realize the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce. A framework to enable regional data transfers will benefit consumers, businesses, and governments. Ministers have endorsed the APEC Privacy Framework, recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region.

17 Similarly, Pt III of the OECD Guidelines addresses the importance of preserving cross-border data transfers and includes the following "basic principles of international application":

> (a) countries should "take into consideration the implications for other [countries] of domestic processing and re-export of personal data";
> (b) countries should "take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through [another] country, are uninterrupted and secure";
> (c) countries should "refrain from restricting transborder flows of personal data between itself and another [country] except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation";
> (d) countries may "impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other [country] provides no equivalent protection"; and
> (e) countries should "avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection".

B. "Do Not Call" provisions

18 One area where the PDPA differs from many other data protection laws is its inclusion of specific provisions regulating certain telemarketing activities. This arises as the PDPA permits organisations to use personal data which were collected before the PDPA's Data Protection Provisions came into force[26] for the purposes for which they were collected, unless the individual has withdrawn consent for such use.[27] In addition, an individual's business contact information[28] is expressly excluded from the scope of the PDPA's Data Protection Provisions.[29] The effect of these provisions is that organisations could continue to use individuals' personal or business contact information (which forms part of their personal data) for telemarketing purposes and individuals would be required to "withdraw consent" for such usage, if they so desired. In its consultation paper for the Second Consultation,[30] MICA noted that having a national DNC registry "provides the individual a simple and effective way to opt-out of all marketing messages without having to withdraw consent for telemarketing from every organisation".[31]

C. Legislative sources

19 MICA's consultation paper for the First Consultation noted that its proposed data protection regime was based on the principles of the Model Code (which was derived from the OECD Guidelines). In addition, reference was made to the data protection laws of certain "key jurisdictions"

---

26 That is, before 2 July 2014.

27 Personal Data Protection Act 2012 (Act 26 of 2012) s 19.

28 Business contact information is defined as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes" (s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012)).

29 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(5).

30 *Consultation Paper on Framework Details for the Establishment of a National Do-Not-Call Registry* (MICA, 31 October 2011).

31 *Consultation Paper on Framework Details for the Establishment of a National Do-Not-Call Registry* (MICA, 31 October 2011) at para 2.5.

such as the EU, the UK, Canada, Hong Kong and New Zealand as well as the APEC Framework.[32]

20 In view of the adoption of the Model Code by various organisations in Singapore, one implicit policy consideration was the extent to which Singapore's data protection law should retain and incorporate, as far as possible and desirable based on other local policy considerations, the principles of the Model Code.[33] In this regard, Canada was a significant reference jurisdiction for the development of the PDPA as its national data protection law, the Personal Information Protection and Electronic Documents Act[34] ("PIPEDA"), incorporated the data protection principles of the CSA Model Code.[35] A few Canadian provinces also passed data protection laws in line with the PIPEDA, which thus incorporated the substance of the CSA Model Code's principles (even if the legislative drafting style differed). Among these, British Columbia's Personal Information Protection Act[36] ("PIPA") was a reference for many of the data protection obligations in Pts III to VI and the Second to Fourth Schedules to the PDPA.[37]

---

32 *Consultation Paper on a Proposed Consumer Data Protection Regime for Singapore* (Ministry of Information, Communications and the Arts, 13 September 2011) at para 3.6.

33 The National Internet Advisory Committee's *Model Data Protection Code for the Private Sector* contained ten data protection principles, namely, Accountability (Principle 1), Specifying Purposes (Principle 2), Consent (Principle 3), Limiting Collection (Principle 4), Limiting Use, Disclosure and Retention (Principle 5), Accuracy (Principle 6), Security Safeguards (Principle 7), Openness (Principle 8), Individual Access and Correction (Principle 9) and Challenging Compliance (Principle 10).

34 SC 2000, c 5.

35 See Sch 1 to the Personal Information Protection and Electronic Documents Act (SC 2000, c 5) (Canada).

36 SBC 2003, Cap 63.

37 See Pts 2–7 and 9 of the Personal Information Protection Act (SBC 2003, Cap 63) (British Columbia, Canada) ("PIPA"). Part 8 of PIPA (concerning administration of the access and correction requirements in Pt 7) was a general reference for Pt II of the Personal Data Protection Regulations 2014 (S 362/2014) which similarly concerns administration of the access and correction obligations in Pt V of the Personal Data Protection Act 2012 (Act 26 of 2012).

21 One area where the PDPA differs from the PIPEDA and the PIPA is in relation to its treatment of data intermediaries, which are defined in the PDPA as organisations which process personal data on behalf of another organisation ("data controller").[38] The concept of a data intermediary is not expressly referred to in the Canadian legislation. MICA's policy intent was to limit the obligations of data intermediaries in view of the differing degree of control they have over the personal data they are processing, as compared to the data controllers.[39] In developing the concept of a data intermediary for the purposes of the PDPA, reference was made to the concept of a data processor under the EU Directive and the UK's Data Protection Act 1998[40] ("DPA"). Taking into account local needs and policy considerations, data intermediaries are only required to comply with ss 24 and 25 of the PDPA (relating to protection and retention of personal data respectively) and data controllers are instead responsible for the data processing activities of their data intermediaries.[41]

22 While data protection laws generally cover the use of an individual's personal and business contact information for telemarketing purposes (that is, as part of the use of an individual's personal data), few include express provisions regulating such uses. For example, the UK's DPA provides for an individual's right to prevent processing (use) of his personal data for purposes of direct marketing[42] and Hong Kong's Personal Data (Privacy) Ordinance[43] has extensive provisions on the use of personal data in direct marketing.[44] The PDPA adopts a somewhat intermediate approach with the establishment of the national DNC registry and provisions which require organisations to check the DNC registry if they intend to send

38 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

39 See *Consultation Paper for the Proposed Personal Data Protection Bill* (MICA, 19 March 2012) at paras 2.23–2.25.

40 c 29.

41 Personal Data Protection Act 2012 (Act 26 of 2012) ss 4(2) and 4(3).

42 Data Protection Act 1998 (c 29) (UK) s 11(1). Also see Art 14(b) of the EU Directive. The term "direct marketing" generally refers to the sending of marketing or advertising material to particular individuals. For example, see s 11(3) of the UK Data Protection Act 1998.

43 ER 1 of 2013 (Cap 486).

44 Personal Data (Privacy) Ordinance (ER 1 of 2013) (Cap 486) (Hong Kong) Pt 6A.

certain telemarketing messages to a Singapore telephone number[45] or make a voice call containing a telemarketing message to a Singapore telephone number ("Do Not Call Provisions").[46] Under the Do Not Call Provisions, organisations are not permitted to send such messages or make such voice calls unless the telephone number is not registered on the DNC registry[47] or they have obtained the individual's "clear and unambiguous" consent.[48]

23 One local reference for the PDPA's Do Not Call Provisions was the Spam Control Act[49] ("SCA"). The SCA governs the sending of unsolicited commercial electronic messages, which overlaps with the concept of a "specified message" in the PDPA.[50] While there are some similarities, there are also notable differences between the PDPA's Do Not Call Provisions and the provisions of the SCA. For example, the SCA focuses on messages sent "in bulk"[51] whereas the PDPA has a broader scope and also covers messages sent to a single individual or few individuals. In addition, the coverage of the modes by which messages are sent differs between the two Acts.[52] Ultimately, as noted in MICA's consultation paper for the Second

45 The term "Singapore telephone number" is defined to refer to telephone numbers that are in accordance with Singapore's National Numbering Plan (s 36(1) of the Personal Data Protection Act 2012 (Act 26 of 2012)).

46 The telemarketing messages which are subject to the "Do Not Call" provisions of the Personal Data Protection Act 2012 (Act 26 of 2012) are referred to in the Act as "specified messages". These are defined in s 37.

47 Organisations must also comply with the requirements of the rest of the Personal Data Protection Act 2012 (Act 26 of 2012) including, for example, obtaining an individual's consent for use of his telephone number for marketing purposes, unless use without consent is permitted or authorised under any written law (see s 13).

48 Personal Data Protection Act 2012 (Act 26 of 2012) ss 43(1) and 43(3). The Personal Data Protection Act 2012 also includes obligations to include certain contact information in the telemarketing message and, in the case of voice calls, to not conceal or withhold their calling line identity (ss 44 and 45).

49 Cap 311A, 2008 Rev Ed.

50 See the definition of a "commercial electronic message" in the Spam Control Act (Cap 311A, 2008 Rev Ed) (s 3) and the definition of "specified message" in the Personal Data Protection Act 2012 (Act 26 of 2012) (s 37).

51 See ss 6(1) and 11 of the Spam Control Act (Cap 311A, 2008 Rev Ed).

52 The Spam Control Act (Cap 311A, 2008 Rev Ed) covers messages sent to an electronic mail address or a mobile telephone number (see s 2(1), definitions of "electronic address", and s 4, definition of "electronic message"). This

(*continued on next page*)

Consultation, the scope of the PDPA's Do Not Call Provisions is not the same as the scope of the SCA and accordingly it was decided that the SCA would continue to apply.[53]

III. Conclusion

24 Data protection law is an evolving field. While there is, as yet, no global instrument or treaty on data protection (beyond regional instruments such as the EU Directive), international bodies such as APEC and the OECD are active in their efforts to achieve a broad consensus among their members on the key elements and requirements of privacy and data protection.[54] There is a highly anticipated update to the EU's data protection regime, in the form of its General Data Protection Regulation,[55] which will come into force and supersede the EU Directive in May 2018. Within the Association of Southeast Asian Nations ("ASEAN"), the ASEAN Telecommunications and Information Technology Ministers Meeting ("TELMIN") entered into a *Framework on Personal Data Protection* on 25 November 2016 ("ASEAN Framework"). The ASEAN Framework aims to strengthen the protection of personal data within ASEAN and facilitate co-operation among participating Member States,

---

would cover messages sent by electronic mail or text message but not voice calls. The Personal Data Protection Act 2012 (Act 26 of 2012), on the other hand, covers messages sent to a Singapore telephone number (see s 36(1), definitions of "message" and "send"), which generally includes both fixed-line and mobile telephone numbers. Hence, the Personal Data Protection Act 2012 covers messages sent by way of text message or a facsimile transmission, as well as voice calls.

53 *Consultation Paper on Framework Details for the Establishment of a National Do-Not-Call Registry* (MICA, 31 October 2011) at paras 4.5 and 4.6.

54 For more information, see the websites of the APEC Electronic Commerce Steering Group (<www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group>) and the OECD Directorate for Science, Technology and Innovation on privacy (<www.oecd.org/sti/ieconomy/privacy.htm>).

55 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC.

"with a view to contribute to the promotion and growth of regional and global trade and the flow of information".[56] In addition to international developments, technological developments are continuing unabated and will present new challenges, perhaps requiring new answers, in relation to data protection. In this regard, Singapore has taken a significant step with the enactment of the PDPA and it has joined the global discourse on how countries and societies can and should facilitate innovation, development and economic growth while protecting individuals' rights to their personal data.

56 *ASEAN Framework on Personal Data Protection* at para 1.

A SURVEY ON ENFORCEMENT OF THE PERSONAL DATA PROTECTION ACT 2012*

LIM Chong Kin†
LLB (Hons) (National University of Singapore),
LLM (National University of Singapore);
Advocate and Solicitor (Singapore), Solicitor (England & Wales)

Charmian AW‡
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore); CIPP/E, CIPP/A

1 Since the introduction of the Personal Data Protection Act 2012[1] ("PDPA") some three years ago, there have been a number of significant and noteworthy developments that have underscored the need for a strong and robust data protection regime in Singapore.

2 Chief among these would be Singapore's Smart Nation programme, which plans involve making Singapore a nation of smart technology and

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Director; Head, Competition & Regulatory Practice Group; Head, Telecoms, Media & Technology Practice Group, Drew & Napier LLC. Chong Kin is widely regarded as a pioneer and leading practitioner on TMT, competition and regulatory and data protection work. Amongst others, he has won plaudits in Asia Pacific Legal 500; Chambers Asia Pacific: Band 1 for TMT; and has been endorsed for his excellence in regulatory work: Practical Law Company's Which Lawyer Survey; Who's Who Legal: TMT and Who's Who Legal: Competition.

‡ Director, Telecoms, Media & Technology Practice Group, Drew & Napier LLC. Charmian is recommended for corporate-related TMT and data privacy work by Asia Pacific Legal 500, and a Leading Lawyer in Who's Who Legal TMT. She is a Certified Information Privacy Professional (Europe) (CIPP/E) and Certified Information Privacy Professional (Asia) (CIPP/A), and is currently a co-chair of the International Association of Privacy Professionals' KnowledgeNet chapter in Singapore.

1 Act 26 of 2012.

innovation by harnessing technology and data to improve and enhance the way in which its citizens live, work, play and interact. As the use of digital technology such as cloud computing, the Internet of Things and big data analytics become increasingly pervasive in our social and economic activities as well as in our private and civic lives, the risks and impact posed by cybersecurity breaches have also become more pronounced.

3 It is against this backdrop that the need to ensure responsible use of personal data in connection with the adoption of new technologies is now more critical than ever. It is of growing importance that all stakeholders in Singapore's data eco-system instil a culture of accountability that goes beyond mere compliance with applicable law.

4 It is therefore apt and relevant to examine the topic of enforcement of the PDPA. One of the primary aims of enforcement would be to send a clear signal to businesses as to the level of compliance which they are expected to adopt, in ensuring the effectiveness of our data protection laws.

5 In this article, we will first take stock of the enforcement decisions which have been made by the Personal Data Protection Commission ("PDPC") to date, and attempt to draw out some general principles as to how the PDPC has interpreted and applied the PDPA thus far.

6 We will then consider some potential areas in which enforcement of the PDPA could be expected to evolve in the future, taking into account current trends in data protection enforcement and regulatory regimes in other parts of the world.

7 Finally, we will conclude with our brief thoughts on the way forward for Singapore, in the context of our unique approach to data protection and law enforcement generally.

I. The Personal Data Protection Commission's enforcement decisions to date

8 The PDPC has been relatively active in its enforcement of the PDPA.

9 As of February 2017, the PDPC has received about 1,300 complaints alleging that the PDPA had been breached by various organisations. Out of these, the majority (71%) comprise isolated or minor concerns which were handled by facilitation between complainants and organisations while 19% of these were resolved via investigations by the PDPC. At the time of

writing this article, the PDPC has published 23 data protection enforcement decisions, setting out the enforcement actions taken by the PDPC against the organisations and the factors and considerations taken into account by the PDPC in coming to its decision.

10 It is somewhat apparent from the PDPC's enforcement decisions that, despite the transition period of 18 months from the inception of the PDPA for organisations to phase in the new law and the various guidelines issued by the PDPC, many organisations still appeared to lack an overall awareness and sensitivity to the data protection obligations under the PDPA ("Data Protection Obligations"), and in particular, the Protection Obligation.

11 In a number of the enforcement decisions, organisations were not even aware that a data breach had occurred until they were informed of the same during the PDPC's investigations. That said, it is interesting to note that most of the enforcement decisions were initiated by complaints from members of the public, which perhaps demonstrates a growing public awareness of an individual's rights under the PDPA.

12 By and large, the data breaches in the enforcement decisions to date have not been particularly severe, and the organisations involved have mostly been small-medium enterprises ("SMEs"). Given the increasing number of data attacks reported globally, however, it may be likely that the impact of data breaches would become greater, with larger organisations in Singapore being affected as well in time.

13 Broadly speaking, the PDPC's enforcement decisions demonstrate its approach towards the enforcement of the PDPA. We discuss some of these on a non-exhaustive basis.

14 Firstly, in relation to the construction of the term "personal data" under the PDPA, the PDPC appears to have adopted a purposive stance. For instance, the PDPC has held that information leaked could constitute personal data even if it was protected by encoded passwords because the passwords were encoded with a commonly used cryptographic hash function which could be deciphered easily.[2] In a number of cases where the PDPC did not find any breach of the Data Protection Obligations,[3] the

2 *Fei Fah Medical Manufacturing Pte Ltd* [2016] SGPDPC 3 at [19]–[20].

3 In relation to complaints made against Interflour Group Pte Ltd and Black Peony.

PDPC has also considered that e-mails and private communications such as WhatsApp messages and chats do not necessarily constitute personal data *per se*.

15 In relation to consent, the PDPC's enforcement decisions reveal that the PDPC has been willing to scrutinise the *scope* of consent (both express and deemed) given by the individual, in determining whether the organisation had complied with the Consent Obligation under the PDPA.[4]

16 The PDPC's enforcement decisions have also been useful in providing details as to how organisations have failed to fulfil the Protection Obligation, such as by specifying the areas in which a breaching organisation's security arrangements were lacking. Specifically, it appears that the PDPC has been prepared to enforce the PDPA even in cases where the data breaches do not affect a large number of individuals.[5]

17 With regards to data intermediaries, the PDPC has also taken the position that organisations should be held responsible for the actions of their vendors where these vendors have been engaged to process personal data on behalf of the organisations. In fact, even where the breaches were shown to have been directly caused by the vendor/data intermediary's failure to make reasonable security arrangements to protect the personal data,[6] the PDPC has in its enforcement decisions emphasised the need for the engaging organisations to take active steps in ensuring that an appropriate level of security is accorded to personal data processed by their intermediaries. Such steps include having a sufficient understanding of the vendors, as well as working closely with them to ensure that personal data which is processed on the organisations' behalf is protected in accordance with the PDPA. To this end, the PDPC has published several helpful guides to assist SMEs in improving their personal data management and security

4 *AIA Singapore Pte Ltd* [2016] SGPDPC 10, see also the Personal Data Protection Commission's treatment of the complaints against Savills Residential Pte Ltd; and Asia Renal Care (Katong) Pte Ltd and Fresenius Medical Care Singapore Pte Ltd.

5 *Eg*, *Chua Yong Boon Justin* [2016] SGPDPC 13 and *Universal Travel Corp Pte Ltd* [2016] SGPDPC 4.

6 *K Box Entertainment Group Pte Ltd and Finantech Holdings Pte Ltd* [2016] SGPDPC 1; *Challenger Technologies Ltd and Xirlynx Innovations* [2016] SGPDPC 6; *Fu Kwee Kitchen Catering Services and Pixart Pte Ltd* [2016] SGPDPC 14.

practices, including the *Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data*,[7] and the Guide to Building Websites for SMEs.[8]

18 That said, the PDPC will not necessarily penalise an organisation for its data intermediary's failure to protect personal data, if the organisation is able to clearly demonstrate that it has done everything possible to communicate its expectations to the data intermediary but the data intermediary still failed to carry out the necessary security measures.[9]

19 More generally speaking, it may also be comforting for businesses to observe that the PDPC has adopted a pragmatic approach in its interpretation of the exceptions under the PDPA, such as the exclusion of "business contact information" from the applicability of the Data Protection Obligations,[10] and the "publicly available" exception to the Consent Obligation.[11]

20 With regard to the imposition of financial penalties, even though the PDPC has the power to issue a financial penalty of up to $1m, the highest penalty that the PDPC has issued thus far is $50,000.[12] In most of the other cases, the PDPC has issued relatively modest financial penalties of between $500 and $25,000 or a warning. This is commensurate with the fact that most of the data breaches have not been particularly severe and the organisations involved were SMEs. The PDPC has also demonstrated flexibility in its enforcement measures, and has in several cases delivered warnings to organisations in breach of the Data Protection Obligations, in lieu of issuing financial penalties or directions to take remedial action. In cases where a breach could not be clearly established, this has also not prevented the PDPC from issuing advisory notices to organisations.

---

7 20 July 2016.

8 Updated on 20 January 2017.

9 *Central Depository (Pte) Ltd and Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC 11; *Aviva Ltd and Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC 15.

10 *Eg*, *Comfort Transportation Pte Ltd and CityCab Pte Ltd* [2016] SGPDPC 17 and in relation to the complaint against MyTuitionClub Pte Ltd.

11 In relation to complaints made against Selby Jennings and Strategem Global Recruitment Pte Ltd.

12 *K Box Entertainment Group Pte Ltd and Finantech Holdings Pte Ltd* [2016] SGPDPC 1.

21 It will be interesting to see how cases may arise from other types of breaches of the PDPA in future, and in particular, how the PDPC will apply and enforce the Transfer Limitation Obligation in the context of a globalised economy where more and more economic and social activities are taking place online, such that cross-border data transfers are increasingly commonplace and play a key role in businesses today.

22 It is also noteworthy that the full range of the PDPC's powers has yet to be tested and used. For example, there are certain requirements under the PDPA that would amount to criminal offences, and legal proceedings may be taken to enforce a direction once the PDPC has registered a direction under s 28(2) or 29 of the PDPA in the District Court. It will be interesting to see how and in what circumstances the PDPC will invoke those powers, particularly if there is a breach of the PDPA involving any part of Singapore's critical information infrastructure.

23 To date, there has also only been one appeal against the imposition of a financial penalty brought before the Data Protection Appeal Committee ("DPAC") by the Institution of Engineers Singapore, and that appeal was dismissed in its entirety.[13] No further appeal against the decisions of an Appeal Committee has been made to the High Court and Court of Appeal on points of law and/or on the amount of the financial penalty. It therefore remains to be seen how the Singapore courts will decide on an appeal of a decision made by the DPAC.

II. Possible areas of development

24 As Singapore's data protection regime continues to develop alongside a national cybersecurity legislation which is expected to be passed later this year, it will be crucial for all organisations to play their part in safeguarding personal data in their control or possession, in order for Singapore to maintain its credibility as a trusted technology hub and choice location for data processing services.

13 The grounds of decision for the appeal have not been published as at the time of writing.

A. Sensitivity of personal data and severity of data breaches

25 In this connection, the PDPC may consider fine-tuning and adopting an even more robust stance towards certain breaches of the PDPA.

26 For instance, while the PDPA does not specifically define "sensitive personal data" (unlike in jurisdictions such as the US, the UK and Australia), there may be an increasing acknowledgment of specific categories of "more sensitive" personal data, which typically includes medical records and bank account details.

27 There may also be an increasing recognition of the severity of consequences of a data breach, for instance, where there is a risk of identity theft, credit card or other fraud, and cybercrime.

28 There are already some indications of the PDPC leaning towards such an enforcement approach. The PDPC's *Advisory Guidelines on Enforcement of the Data Protection Provisions* ("Enforcement Guidelines"),[14] for instance, currently provide that the PDPC will take into account certain factors, including the seriousness and impact of such breach, in considering whether to direct an organisation to pay a financial penalty for a breach of any Data Protection Obligation. In addition, the Enforcement Guidelines state that the PDPC may impose a higher financial penalty on an organisation if its breach of a Data Protection Obligation affects sensitive personal data.

29 While "sensitive personal data" is not defined further in the PDPA, the Enforcement Guidelines do indicate that, if the breaching organisation is in the business of handling large volumes of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to a person (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such personal data, the PDPC may consider this to be an aggravating factor in meting out penalties.

30 Recent enforcement decisions have also seen the PDPC taking into account the sensitivity of the personal data, in assessing the appropriate

14 21 April 2016.

directions to be imposed on organisations in violation of the Data Protection Obligations.[15]

B. Data breach reporting/notification

31 In jurisdictions such as the US, there is also a requirement for organisations to report data security breaches or losses to the affected individuals, credit bureaus, State Attorney Generals and/or other state officials in certain instances, depending on applicable state laws and/or severity of the breaches.

32 Currently, the Enforcement Guidelines indicate that the PDPC may, in calculating the financial penalty to be imposed on organisations in breach of the PDPA, consider the fact that an organisation had provided timely notification of its breach to affected individuals and/or the PDPC to be a mitigating factor.

33 In a similar vein, the PDPC's *Guide to Managing Data Breaches*[16] also encourages organisations to notify individuals affected by a data breach and/or report a data breach incident to the PDPC. If the data breach involves sensitive data, organisations are also advised to notify other relevant third parties such as the police, banks and credit card companies. However, it is not mandatory under the PDPA for organisations to do so.

34 The PDPC may therefore consider implementing mandatory reporting of data breaches, or placing greater emphasis on the reporting of data breaches in its future enforcement decisions. Such a move would represent a shift from mere compliance to accountability, and may therefore compel organisations to pay closer attention to their obligations under the PDPA.

35 At the same time, alerting affected individuals and/or other relevant third parties would also enable them to take preventive measures early, to minimise the impact of the data breach.

---

15 *Eg*, *Central Depository (Pte) Ltd and Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC 11 and *Aviva Ltd and Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC 15.

16 8 May 2015.

36 Notwithstanding, it is important to bear in mind that such mandatory reporting requirements may prove onerous for some organisations, which would have to devote more resources to ensuring that their systems and processes are sufficiently well equipped and robust enough to monitor and detect data breaches, so as to enable them to notify the relevant parties on a timely basis.

C. Alternative dispute resolution

37 Given that enforcement of the PDPA is still at a relatively early stage, it would be beneficial for the PDPC to continue issuing enforcement decisions in respect of breaches of the PDPA, especially where a novel point is involved, in order to provide organisations with guidance as to the standards of data protection compliance required.

38 Moving forward, as the data protection regime in Singapore matures and the PDPC builds up its body of enforcement decisions, the PDPC may wish to place greater focus on the adoption of alternative dispute resolution. Alternative dispute resolution mechanisms may be an attractive alternative to organisations that wish to avoid the reputational implications that may arise from a publication of an enforcement decision. Such measures may also encourage more openness and transparency between organisations and individuals in the resolution of less severe breaches of the PDPA.

39 By way of illustration, in Hong Kong, most complaints of a breach of the Personal Data (Privacy) Ordinance[17] are resolved without the need for the Privacy Commissioner for Personal Data to issue an enforcement notice because organisations typically agree to provide an undertaking to change its practices and sometimes offer compensation to affected individuals.

40 At present, the PDPC has indicated in its Enforcement Guidelines that it will typically consider whether a complaint may be more appropriately resolved by other means, before deciding whether or not to commence an investigation. For example, the PDPC may, with the consent of both the individual complainant and the organisation, refer the case for mediation.

17 Cap 486.

41 In addition, the PDPC is empowered to direct the complainant and/or the organisation to attempt to resolve a complaint in the manner directed by the PDPC, regardless of whether the parties have consented to the same. Insofar as a complaint is resolved by way of such measures, the PDPC has indicated that it will generally not proceed with an investigation.

III. The way forward and concluding remarks

42 It is expected that with the emergence of new technologies and new uses of data, data protection regulators around the world may be required to adapt current approaches to the enforcement of their respective data protection laws, in order to address the challenges thrown up by such developments.

43 Similarly, the PDPC may be expected to issue additional guidance, and/or update existing guidelines, to reflect its enforcement policies as they evolve and develop. In doing so, it would be important for the PDPC to balance the competing interests of consumers who desire to see greater protection of their personal data and businesses who are concerned that overly stringent protection regimes will unduly restrict their business activities and create obstacles to trade and innovation.

44 The authors expect that as our personal data protection laws move in tandem with Singapore's aspirations of being the world's first true Smart Nation, there will be even closer and greater collaboration between all the relevant stakeholders, and the PDPC will continue to work alongside the other divisions in the Info-communications Media Development Authority ("IMDA") and other regulators that oversee other integral parts of Singapore's data eco-system. Without limitation, these other regulators include the recently set up Cyber Security Agency, GovTech, the Monetary Authority of Singapore for the banking sector, and other sectoral regulators.

45 In relation to international co-operation, this will be of critical importance to Singapore as the world becomes increasingly digital and cross-border transfers of data become more pervasive than ever before. In a world where data centres and servers are located all over the world, the need for an internationally compatible data protection regime is not just important for the protection of personal data but also for international trade and data mobility for consumers. Hence, the authors would also expect that there will be keen co-operation and tie-ups between Singapore

and its regional and international partners, including Interpol, ASEAN and IMDA's regional and international counterparts.

PERSONAL DATA PROTECTION ACT 2012: UNDERSTANDING THE CONSENT OBLIGATION*

YIP Man†
LLB (Hons) (National University of Singapore), BCL (Oxford); Advocate and Solicitor (Singapore)

I. Introduction

1 The Personal Data Protection Act 2012[1] ("PDPA") provides the baseline standards of protection of personal data and works in tandem with existing law to provide comprehensive protection. The birth of the legislation clearly signals Singapore's commitment to protect the collection, use and disclosure of personal data in the age of big data and its awareness of the importance of such protection in strengthening Singapore's position as a leading commercial hub. Significantly, the PDPA protection model balances "both the rights of individuals to protect their personal data" against "the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes".[2] The approach is thus a pragmatic one. The legislation does not promise uncurtailed protection of informational privacy of the individual, a model that would be practically difficult to

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of her employer. All errors remain the author's own.

† Associate Professor of Law, School of Law, Singapore Management University; DS Lee Foundation Fellow. Yip Man is a Panel Speaker on "Restitution" for the Attorney-General's Chambers' Professional Development Programme, the Asia Pacific Digest Editor for the Restitution Law Review and a co-Administrator of the Singapore Law Blog. She previously served as a member of the Singapore Academy of Law Law Reform Committee.

1 Act 26 of 2012.

2 Personal Data Protection Commission website <https://www.pdpc.gov.sg/legislation-and-guidelines/overview> (accessed 7 January 2017). The word "organisation" is defined under s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) to include "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".

enforce, as well as lead to the creation of a trade barrier. Nor does stringency guarantee better protection in every case.[3]

2 This article examines the role and concept of consent under the PDPA. It shows that the PDPA does not – and rightly so – overemphasise the role of consent in personal data protection. The discussion consists of three main parts. First, at a general level, we consider the significance of consent in personal data protection from both theoretical and practical perspectives. Second, we scrutinise the place of "consent" in the structural framework of the PDPA. Finally, we examine recent decisions delivered by the Personal Data Protection Commission ("PDPC") to gain a better understanding of the enforcement of the consent obligation in practice.

II. Theory of consent in personal data protection

3 Consent is a fundamental legal concept. It is a core requirement of many legal activities, such as the formation of contract, the creation of trust and the transfer of rights. Conversely, the lack of consent for certain acts can lead to legal liability. Consent, as a trigger for a legal event, accords respect to individual autonomy. In the context of personal data, consent operates as a mechanism of authorisation.[4] The requirement of an individual's consent confers control on the individual over the use of his personal data by others.

4 Accordingly, consent should play an important role in any personal data protection legislation. Yet, the theory of consent presupposes that the individual is always able to make a voluntary, informed choice. Consent in practice is likely to present a different picture. It has been forcefully argued that "an overemphasis of autonomous authorisation" will lead to an overload of consent transactions[5] with the consequence that consumers suffer from "consent fatigue" and "consent desensitisation", thereby ultimately weakening the consent mechanism as an effective way of seeking

3 See Bart Willem Schermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171.

4 See Bart Willem Schermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171 at 174–175.

5 This problem is particularly acute in the context of Internet activities.

voluntary, intentional and informed authorisation.[6] Alternative models have thus been proposed, including paternalism (banning certain kinds of dealings with personal data); making privacy notices more reasonable and accessible to ensure informed and voluntary choices;[7] and a differentiated consent model where the type of consent required is based on the severity of risks/dangers associated with the particular kind of transaction.[8]

5 Further, the role (and degree of emphasis) of consent within the regulatory framework should be assessed by considering the other interests that are worth protecting. An overemphasis on consent in personal data protection law would undoubtedly lead to higher compliance costs for businesses and slower transaction rates. These consequences would affect both organisations as well as individuals. Beyond purely economic consequences, organisations may require an individual's personal data for legitimate and/or reasonable activities. To accord full control to individuals in deciding whether their personal data may be collected, used or disclosed can have serious impact upon the functioning of social and legal relationships.

6 Next, we turn to examine the role and concept of consent under the PDPA. The analysis shows that the Singapore protection model does not overly emphasise consent. Instead, it embodies a balancing approach that incorporates principles of necessity, reasonableness and fairness.

---

6 Bart Willem Schermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171 at 176–179.

7 Aleecia M McDonald & Tom Lowenthal, "Nano-notice: Privacy Disclosure at a Mobile Scale" (2013) 3 *Journal of Information Policy* 331.

8 Bart Willem Schermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171.

III. Role and concept of consent under the Personal Data Protection Act

A. Concept of consent

7 As a general rule, the PDPA prescribes that an organisation requires consent from the individual to collect, use or disclose personal data relating to that individual. Section 13 of the PDPA provides as follows:

> An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless —
>
> (*a*) the individual *gives, or is deemed to have given, his consent* under this Act to the collection, use or disclosure, as the case may be; or
>
> (*b*) the collection, use or disclosure, as the case may be, without the consent of the individual is *required or authorised under this Act or any other written law*.
>
> [emphasis added]

8 Relevantly, the meaning of "consent" is not defined in the PDPA. This may raise concerns of uncertainty. However, there is ample guidance under the PDPA when one turns to look at other provisions. Valid consent can only be obtained from an individual, as a general rule, if the individual has been notified of the purposes for the collection, use or disclosure pursuant to s 20.[9] Section 14 provides that consent that is obtained pursuant to deceptive or misleading practices is invalid. Clearly, both s 14 and s 20 are inserted to ensure that consent is given on an *informed* basis. Another limit, imposed by s 18(2), is that personal data may only be collected, used or disclosed for purposes "that a reasonable person would consider appropriate in the circumstances".[10] Section 11(1) further clarifies that "[i]n meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances". The lack of definition is not always a shortcoming: it affords latitude for deciding on a "case-by-case" basis and enables the PDPA to better respond to future technological advancements.

---

9 See ss 14(1)(*a*) and 18(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012).

10 This means that appropriateness of purpose is determined objectively.

9 Section 13 also makes clear that consent may be *deemed*. Section 15(1) of the PDPA provides that there is deemed consent by an individual to the collection, use or disclosure of his personal data by an organisation for a purpose if the individual "voluntarily provides the personal data to the organisation for that purpose"[11] or it is *reasonable* that he would do so voluntarily.[12] Section 15(2) continues to provide that if an individual has consented or is deemed to have consented to an organisation disclosing his personal data to another organisation for a particular purpose, the individual is deemed to have consented to the disclosure of the data for that particular purpose by the other (receiving) organisation. Of course, the concept of deemed consent is subject to the limitations imposed by s 18 discussed above, namely, notification of purpose as well as reasonableness of purpose.

10 As a matter of principle, "deemed consent" is not actual consent and may seemingly undercut the control which the PDPA confers upon an individual over the collection, use or disclosure of his personal data. However, in practice, "deemed consent" is a cost-effective means for organisations to obtain authorisation. "Deemed consent" may also benefit the individual in terms of transactional efficiency, as it can reduce consent requests and avoid an overload of consent transactions. Besides, the concept of "deemed consent" is properly circumscribed in the PDPA. Where the individual *voluntarily* supplies personal data to an organisation for a purpose, it is generally fair and reasonable for the individual to be treated as having consented to the collection, use and disclosure of the personal data by the organisation for that purpose. For example, a patient who supplies his personal data to a medical clinic for the purpose of making a medical appointment would be deemed to have consented to the medical clinic's collection or use of his personal data for the purpose of seeking medical treatment.[13] It may even be said that consent could be *inferred* in such circumstances.

11 Greater uncertainty may arise in respect of s 15(1)(*b*) – "it is reasonable that the individual would voluntarily provide the data". But

11 Personal Data Protection Act 2012 (Act 26 of 2012) s 15(1)(*a*).

12 Personal Data Protection Act 2012 (Act 26 of 2012) s 15(1)(*b*).

13 Kah Leng Ter, "Information Management: Towards Consumer Data Protection Legislation in Singapore" (2012) 24 SAcLJ 143 at 163.

individuals need not be overly concerned. First, the burden of proof rests on organisations to show that there is deemed consent. Secondly, whether the individual would have voluntarily provided the personal data is a matter to be assessed objectively. Thirdly, the concept of deemed consent is subject to the s 18 limitations.[14] The clearest example of deemed consent under s 15(1)(*b*) would be where a patient seeks or agrees to a referral by his family doctor to a specialist for further medical treatment. For that purpose, the personal information relating to the individual will need to be disclosed to the specialist clinic and consent for disclosure could be deemed in such circumstances.

12 Finally, s 16 of the PDPA provides that consent (including deemed consent) may be withdrawn.[15] The withdrawal of consent operates prospectively: it does not render the prior collection, use or disclosure of personal data unauthorised. The provision for withdrawal of consent provides further control to the individual to decide how his personal data may be used and such control is particularly crucial in situations of deemed consent.

B. Exceptions

13 Section 13(*b*) provides that the consent of the individual is not required in circumstances where the collection, use or disclosure of personal data is statutorily mandated or authorised. We will focus on statutory authorisation under the PDPA. But before that, it should not be missed that s 4(5) of the PDPA excludes from the scope of Pts III–VI "business contact information"[16] that is not expressly referred to therein. This exclusion is defensible on two grounds. First, business contact information, in most cases, is publicly available information.[17] Secondly, business contact information should not be considered personal data, as it is generated in

14 It is less clear how the notification obligation is to be satisfied in respect of s 15(1)(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012).

15 Note s 16(4) of the Personal Data Protection Act 2012 (Act 26 of 2012).

16 See the definition under s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

17 Exempted under para 1(*c*) of the Second Schedule (collection); para 1(*c*) of the Third Schedule (use); and para 1(*d*) of the Fourth Schedule (disclosure) to the Personal Data Protection Act 2012 (Act 26 of 2012).

connection with and for professional objectives. The point of business contact information is to enable others to contact the individual for professional reasons.

14 More significantly, section 17 of the PDPA provides that personal data can be collected, used and disclosed *without consent* in the circumstances set out in the Second Schedule (collection), Third Schedule (use) and Fourth Schedule (disclosure). These exceptions are generally characterised by necessity, reasonableness and/or fairness. Essentially, the PDPA acknowledges that certain forms of socially, morally or legally acceptable uses of personal data do not require the individual's consent.[18] It has been pointed out that some of the exemptions appear to be very wide,[19] for instance, collection *necessary* for "evaluative purposes"[20] and where the personal data is publicly available.[21] It must nevertheless be borne in mind that an effective control of any form of potential statutory excessiveness is the interpretation and application of the PDPA provisions by adjudicating bodies.

IV. Personal Data Protection Commission decisions

15 The PDPC's decisions on alleged breaches of the consent obligation will be examined in this Part. A number of key points may be drawn from the decisions.

18 Some of these exceptions may overlap with the concept of deemed consent. See, *eg*, para 1(*n*) of the Second Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012).

19 Hannah Lim Yee Fen, "The Data Protection Paradigm for the Tort of Privacy in the Age of Big Data" (2015) 27 SAcLJ 789 at 819–820.

20 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*f*). Also see para 1(*f*) of the Third Schedule and para 1(*h*) of the Fourth Schedule. See the definition of "evaluative purposes" under s 2(1).

21 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*c*); Third Schedule, para 1(*c*); Fourth Schedule, para 1(*d*).

A. Consent

16 The PDPC does not generally object to broadly-worded consent requests[22] or opt-out provisions.[23] The question in each case is whether the relevant provision is effective in seeking consent from the individual in relation to the collection, use or disclosure of his personal data for the relevant purpose. Clear and internally consistent drafting is crucial. In the "absence of clear supporting evidence", the PDPC would, out of prudence, refrain from making a finding of breach.[24]

17 Further, the PDPC does not interpret the concept of "deemed consent" under s 15 widely. In *Universal Travel Corp Pte Ltd*,[25] four passengers sought from the tour agency formal confirmation of cancellation of their flight for the purpose of processing their insurance claims. The tour agency disclosed to each of the four passengers the affected passenger list which contained the four passengers' personal data. The PDPC held that the four passengers could not be deemed to have consented to the disclosure, as each passenger only required his own personal information for the purpose of processing his insurance claim. It was also possible, in the circumstances, for the personal data of the relevant passenger to be released to that passenger alone. Nothing on the facts suggested urgency that would necessitate the dispensation of consent under para 1(*a*) of the Fourth Schedule to the PDPA.

B. Neighbouring obligations

18 The PDPC also emphasised the independence and importance of the "neighbouring obligations"[26] – the notification obligation and the reasonableness of purpose obligation under s 18. The PDPC's approach underscores that the PDPA protection framework is not based solely on consent. In particular, the PDPC said that the reasonableness obligation is "an important aspect of the PDPA as it is effective in addressing excesses in the collection, use or disclosure of personal data" under a broadly-worded

22 See *AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [11]–[12].
23 See *YesTuition Agency* [2016] SGPDPC 5.
24 *AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [12].
25 [2016] SGPDPC 4.
26 *Jump Rope (Singapore)* [2016] SGPDPC 21 at [10].

consent clause.[27] Even if an organisation is not to have breached the consent obligation, it may be guilty of breaching the neighbouring obligations.[28]

19 Interestingly, in *Jump Rope (Singapore)*,[29] the PDPC said that in exceptional circumstances, it may be reasonable for an organisation to disclose personal data of an individual without consent.[30] Such circumstances include the disclosure of personal data of an individual who has been dismissed, blacklisted or undergoing disciplinary proceedings for the purpose of warning others. However, the PDPC said that the organisation must comply with the neighbouring obligations.

C. Exceptions

20 In *My Digital Lock Pte Ltd*,[31] the PDPC considered the "publicly available data", the "necessary for investigations and proceedings" and the "necessary for provision of legal services" exceptions under the Fourth Schedule to the PDPA. In respect of the latter two exceptions, the PDPC stressed that the organisation must show necessity and the disclosure would not be considered necessary for those objectives if there are other ways of achieving the same.[32]

D. Enforcement actions

21 In determining the appropriate enforcement actions to be ordered pursuant to s 29 of the PDPA, the PDPC takes into account a broad range of considerations. The decisions on breach of the consent obligation concerned unauthorised disclosure and the relevant considerations are:

(a) the number of third parties to whom the disclosure has been made;
(b) the period of disclosure;
(c) the amount of personal data disclosed;

27 *AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [18].
28 *AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [19].
29 [2016] SGPDPC 21.
30 *Jump Rope (Singapore)* [2016] SGPDPC 21 at [10]. See also [11] (where notification may be dispensed with).
31 [2016] SGPDPC 20.
32 *My Digital Lock Pte Ltd* [2016] SGPDPC 20 at [21].

(d) the level of sensitivity of the disclosed personal data;
(e) the impact of disclosure upon the individual;
(f) whether the disclosure was caused by wilful or systemic failures of the organisation;
(g) whether the organisation has taken proactive correction procedures; and
(h) whether the organisation has been co-operative in the investigation.

22 In less serious cases,[33] the PDPC issued merely a warning to make clear that breaches of the PDPA are taken seriously. In *Universal Travel Corp Pte Ltd*,[34] the PDPC issued directions for extensive remedial steps to be taken by the organisation for being in breach of s 12 of the PDPA, but it refrained from imposing a fine. In *Chua Yong Boon Justin*,[35] the PDPC imposed a $500 fine on the breaching party on account of the fact that the breach was wilful.[36] However, the PDPC set the fine amount at "the lower end of the spectrum" in view of the fact that the disclosure was limited, one-off, and did not cause a harmful impact on the individual.[37]

V. Conclusion

23 It has been shown in this article that the PDPA, quite rightly, does not overly emphasise the role of consent in personal data protection. It seeks to balance the competing interests of the individual and others who may wish to or require the use of the individual's personal data. It does so through differentiating the type of consent (actual or deemed) that is required based on the risks associated with the transaction and by reference to socially and morally acceptable norms. It also dispenses with the consent requirement in circumstances that are characterised by necessity, reasonableness and/or fairness. Further, the rigours of protection under the

33 See, *eg*, *YesTuition Agency* [2016] SGPDPC 5; *My Digital Lock Pte Ltd* [2016] SGPDPC 20 (also in breach of s 24 of the Personal Data Protection Act 2012 (Act 26 of 2012)) and *Jump Rope (Singapore)* [2016] SGPDPC 21 (also in breach of ss 11 and 20).
34 [2016] SGPDPC 4.
35 [2016] SGPDPC 13.
36 *Chua Yong Boon Justin* [2016] SGPDPC 13 at [19(c)].
37 *Chua Yong Boon Justin* [2016] SGPDPC 13 at [21].

PDPA are not (and cannot be) secured by the consent obligation alone. Other neighbouring obligations, such as the notification and reasonableness of purpose obligations, are also central to the regulatory framework.

FOR ART'S SAKE: THE "ARTISTIC OR LITERARY PURPOSES" EXCEPTION IN THE PERSONAL DATA PROTECTION ACT*

CHEN Su-Anne†
LLB (National University of Singapore);
Advocate and Solicitor (Singapore)

I. Introduction

1 The Personal Data Protection Act 2012[1] ("PDPA") makes it clear that its purpose is to govern the collection, use and disclosure of personal data in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.[2]

2 A key obligation under the PDPA, which goes towards recognising the rights of individuals to protect their data, is the requirement to obtain an individual's consent to the collection, use or disclosure of his personal data ("Consent Obligation"). Without more, this obligation would have enabled an individual to withhold consent to, and effectively prevent, any collection, use or disclosure of any personal data related to him, even if it may be of value to society at large. As with all rights, there has to be a balance involving compromises or limitations. Accordingly, the PDPA sets out various exceptions to the Consent Obligation. One such circumstance is

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of her employer. All errors remain the author's own.

† Deputy Chief Counsel, Personal Data Protection Commission. The author is indebted to Yeong Zee Kin for his invaluable comments which helped refine the draft to this published version. The author would also like to acknowledge the contribution of Charis Seow towards the publication of the article.

1 Act 26 of 2012.

2 Personal Data Protection Act 2012 (Act 26 of 2012) s 3 ("Purpose").

where "the personal data is collected solely for artistic or literary purposes" ("Artistic or Literary Exception").[3]

3 This article explores the possible interpretation and boundaries of the Artistic or Literary Exception, bearing in mind its role in the context of the PDPA.

II. Purpose of the Artistic or Literary Exception

4 In Singapore, the Interpretation Act[4] makes it clear that "[i]n the interpretation of a provision of a written law, an interpretation that would promote the purpose or object underlying the written law shall be preferred to an interpretation that would not promote that purpose or object". With the foregoing in mind, this Part of the article briefly discusses the role of the Artistic or Literary Exception in the context of the PDPA.

5 At the most fundamental level, it is uncontroversial that the genesis of the Artistic or Literary Exception is founded in considerations of freedom of expression.[5] Notably, the Artistic or Literary Exception is but one of several exceptions in the PDPA that goes towards ensuring freedom of expression. The ability to disseminate news is separately preserved by a specific exception to facilitate news activities ("News Activity Exception").[6] There is

---

3 Personal data that are so collected may be used and disclosed for consistent purposes pursuant to paras (1)(*j*) and 1(*s*) of the Third and Fourth Schedules to the Personal Data Protection Act 2012 (Act 26 of 2012) respectively.

4 Cap 1, 1997 Rev Ed.

5 As noted by the then Ministry of Information, Communications and the Arts during the development of the Personal Data Protection Act 2012 (Act 26 of 2012), having this exception "would, on balance, be more in line with international norms": *Public Consultation Issued by Ministry of Information, Communications and the Arts: Proposed Personal Data Protection Bill* (19 March 2012). In this regard, several foreign data protection regimes such as the European Union Directive No 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, which contain a similar exception, expressly make clear that the exception is in furtherance of freedom of expression.

6 It is noted that the News Activity Exception is limited to news activities carried out by "news organisations" as defined in the Personal Data Protection Act 2012 (Act 26 of 2012), such that other organisations must obtain consent

(*continued on next page*)

also a separate exception for publicly available data ("Publicly Available Exception").[7] Collectively, the News Activity Exception and the Publicly Available Exception ensure that newsworthy information and publicly available information can be collected, used and disseminated, to ensure that society continues to benefit from the free flow of information to promote the progress of science and useful arts, and the dissemination of useful knowledge and discoveries.

6 As a third exception that goes towards freedom of expression, it is sensible for the Artistic and Literary Exception to be interpreted in a manner that complements the Publicly Available Exception and the News Activity Exception.[8] From this perspective, in determining the interpretation of the Artistic or Literary Exception, the guiding question could be broadly framed as: "What would constitute artistic or literary purposes that merit an organisation being able to collect, use and disclose personal data, without the individual's consent, where such personal data are not news and not publicly available?"

7 As a general matter, the concept that the arts are intrinsically valuable and should therefore be promoted has been repeatedly recognised in the philosophy of art literature; and likewise, the law has been inclined or obliged to differentiate and confer special protection in respect of the arts.[9] This differentiation is not unique to data protection but has also arisen in

---

if they wish to collect personal data for news activities. It would appear that the balance between rights of individuals and the needs of organisations was intentionally struck in this manner. See paras 1(*h*) and 2 of the Second Schedule to the Personal Data Protection Act 2012.

7 Section 2 of the Personal Data Protection Act 2012 (Act 26 of 2012) defines "publicly available" as "personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event – (*a*) at which the individual appears; and (*b*) that is open to the public". The specific exceptions are set out in para 1(*c*) of the Second Schedule, para 1(*c*) of the Third Schedule and para 1(*d*) of the Fourth Schedule to the Personal Data Protection Act 2012.

8 Having the Artistic or Literary Exception would be "consistent with the complementary exclusion for news activities" (*Public Consultation Issued by Ministry of Information, Communications and the Arts: Proposed Personal Data Protection Bill* (19 March 2012)).

9 Christine Haight Farley, "Judging Art" (2005) 79(4) *Tulane Law Review* 805 at 810.

the context of various other fields such as intellectual property. The boundaries of such differentiation would, however, necessarily vary depending on the particular legislation and the policy intent underlying that legislation. In the context of the PDPA, considering the express purpose as set out in s 3 of the PDPA, the Artistic or Literary Exception should not be interpreted in a manner that unduly circumscribes the right of individuals to determine how their personal data are collected, used and disclosed.

8 With the foregoing in mind, Part III[10] examines the relevant text in the PDPA, and discusses the possible interpretation and boundaries of the Artistic or Literary Exception.

III. Interpretation and boundaries of the Artistic or Literary Exception

A. Ordinary meanings of the terms "artistic" and "literary"

9 The Artistic or Literary Exception in the PDPA is crafted as follows – "the personal data is collected solely for artistic or literary purposes". This begs the fundamental question, "what is an 'artistic or literary purpose'?"

10 Notably, the terms "artistic" and "literary" are not specifically defined in the PDPA. It is therefore apparent that the terms were not intended to take on any specific or exhaustive definition for purposes of the personal data protection regime. As has been recognised by the Personal Data Protection Commission,[11] "it would likely be in line with the purpose of the PDPA for these terms to take on their ordinary meanings. However, … the parameters as to what would constitute 'artistic' purposes may be strongly subjective". In the context of the similar UK exemption for "journalism, art or literature", the UK Supreme Court has also noted that the meaning of "art" in particular has a "striking elasticity".[12]

---

10 See paras 9–15 below.

11 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Photography, Video and Audio Recordings* (revised on 28 March 2017) at para 4.21.

12 Lord Wilson opined that any of the British Broadcasting Corporation's output which did not qualify as journalism would be likely to qualify as literature or

(*continued on next page*)

11 It would appear that the phrase "artistic or literary purpose" is not amenable to a precise definition. Instead, the applicability of the Artistic or Literary Exception would depend on an examination of the facts and circumstances of each case. Nevertheless, in many cases, it would be clear from the context whether or not the Artistic or Literary Exception applies. A police drawing of a suspect would clearly not be for artistic purposes.[13] The collection of an individual's photograph by a prospective employer would also unlikely be for artistic purposes.[14] On the other hand, Andy Warhol's collection of photographic images for his silkscreen painting of individuals, such as Marilyn Monroe, or Colin Davidson's portrait of Ed Sheeran would likely be considered for artistic purposes.[15]

12 Inevitably, there will also be cases in the margins where it would be less clear whether the Artistic or Literary Exception would apply. What if, as a condition to accessing an exhibition, the visitor is to sign and add their fingerprint on a form, with the wording that the visitor agrees to give up the copyright of his fingerprint as printed on the form and assigns this copyright to the organisation. What happens if the completed forms are actually intended to be then displayed on a wall within the exhibition as an installation work of art and also as a record of the audience who had seen the exhibition? This is precisely Carey Young's aptly entitled work, "Artistic Licence".

"in particular, in that its meaning has a striking elasticity – as art". See *Sugar v British Broadcasting Corp* [2012] 1 WLR 439; [2012] UKSC 4 at [38].

13 Other exceptions under the Personal Data Protection Act 2012 (Act 26 of 2012) may apply in such circumstances, such as the exception for investigations in para 1(*e*) of the Second Schedule.

14 Other exceptions under the Personal Data Protection Act 2012 (Act 26 of 2012) may apply in such circumstances, such as the exception for managing an employment relationship in in para 1(*o*) of the Second Schedule.

15 As elaborated further in para 26 below, it will also be interesting to see how the Artistic or Literary Exception interacts with other exceptions and concepts under the Personal Data Protection Act 2012 (Act 26 of 2012).

B. Objective and subjective indicators

13 For situations where it may not be clear whether the Artistic or Literary Exception applies, cases suggest that the following two key indicators[16] may assist in the determination:

> (a) Subjective intent – Whether the intention of the person collecting the personal data is to create a work of artistic or literary expression, as evidenced or corroborated by his conduct.
> (b) Objective purpose – Whether the objective purpose of the work capturing the personal data is for artistic or literary expression, as opposed to a functional or utilitarian purpose.

14 It is further suggested that the subjective intent is the threshold question to be answered, but which has to be buttressed by the objective purpose. An assessment of the objective purpose of the work, as opposed to solely the subjective intent of the person collecting the personal data, would better ensure that the rights of individuals under the PDPA are not unduly circumscribed. To illustrate, if the purpose for collecting personal data was for contract drafting, without more, the exception should not apply even if a person subjectively considered his contract drafting to have artistic or literary value and purpose.

15 Part IV[17] will elaborate further on the first indicator, and Part V[18] will discuss the second indicator in greater detail.

IV. Subjective intent

16 This indicator envisages an assessment of the subjective intent of the person collecting the data and whether it is to create a work of artistic or literary expression. The intent of a person will have to be evidenced or

16 See *Lucasfilm Ltd v Ainsworth* [2009] FSR 2; [2008] EWHC 1878 (Ch), [2010] 1 Ch 503; [2009] EWCA Civ 1328, [2012] 1 AC 208; [2011] UKSC 39; see also, Henry Lydiate, "What is Art? A Brief Review of International Judicial Interpretations of Art in the Light of the UK Supreme Court's 2011 Judgment in the Star Wars Case: *Lucasfilm Limited v Ainsworth*" (2011–2013) 4 J Int'l Media & Ent L 111; Leonard D DuBoff, "What is Art? Toward a Legal Definition" (1989) 12 Hastings Comm & Ent LJ 303.

17 See paras 16–18 below.

18 See paras 19–37 below.

corroborated by his conduct, such as declarations by the person of his intent when he was collecting the personal data, or whether he offered his work for sale in an art gallery, *etc*. Other cases may, of course, involve a more detailed examination of the conduct of the creator.

17 To illustrate, in a New York Customs Court trial between the US Customs and Constantin Brancusi[19] (often referred to as the patriarch of modern sculpture), the US Customs sought the payment of import duty on Brancusi's impressionistic bronze sculptures entitled "Bird in Space" but in respect of which "difficulty might be encountered in associating it with a bird". In determining whether Brancusi's sculpture was a work of art and therefore to be accorded duty-free status (not being in direct competition with American goods), the court's decision depended heavily on the intentions of Brancusi who explained that his intent was to capture the essence of flight in his sculptures, and gave evidence of how he executed his work, including how he had to take a long time to "polish the bronze with files and very fine emery" to achieve the "artistic finishing".

18 Where the threshold question of whether the subjective intent of the organisation collecting the personal data is for artistic or literary purpose is met, this in itself should not be conclusive that the Artistic or Literary Exception applies. Given that this exception would effectively enable an organisation to collect, use and disclose personal data without the individual's consent, the objective purpose of the work in issue should also be assessed, as elaborated in Part V[20] below.

V. Objective purpose

A. "Artistic works" or "literary works"

19 This indicator involves a determination of whether the objective purpose of the work capturing the personal data is for artistic or literary

19 *Brancusi v United States* 54 Treas Dec Cust 428 (Cust Ct 1928), referred to in Henry Lydiate, "What is Art? A Brief Review of International Judicial Interpretations of Art in the Light of the UK Supreme Court's 2011 Judgment in the Star Wars Case: *Lucasfilm Limited v Ainsworth*" (2011–2013) 4 J Int'l Media & Ent L 111 at 124–125.

20 See paras 19–37 below.

expression, as opposed to a functional or utilitarian purpose. Simply put: "Is the work an artistic or literary work?"

20 In this regard, it is clear from the background, context and underlying intent of the PDPA that it was not intended to adopt wholesale the definitions of the terms "artistic works" and "literary works" in the Copyright Act.[21] Neither the PDPA nor any other foreign data protection laws the author has surveyed have adopted or adapted the definitions in the copyright regime. In particular, it would not be appropriate to consider the collection of personal data for creating any "artistic work" or "literary work", as defined in the Copyright Act, to automatically fall within the Artistic or Literary Exception of the PDPA. Taking such an approach would have the undesirable consequence of all personal data captured in photographs, compilations, *etc*, being considered as falling within the exception.[22] Such a reading of the Artistic or Literary Exception would severely circumscribe the application of the PDPA.[23]

---

21 Cap 63, 2006 Rev Ed. Understandably, questions have often been raised about how the Artistic or Literary Exception in the Personal Data Protection Act 2012 (Act 26 of 2012) corresponds to the terms "artistic works" and "literary works" in the Singapore Copyright Act, where the terms have traditionally been important. This article is not, however, intended to be a comprehensive analysis of the interaction issues between the Personal Data Protection Act and Copyright Act, or of the extent of overlap between the Artistic or Literary Exception under the Personal Data Protection Act and the categories of works covered under the Copyright Act.

22 The terms "artistic work" and "literary work" are given specific definitions under the Copyright Act (Cap 63, 2006 Rev Ed) that differ from the ordinary meaning of these terms. For example, "artistic works" under the Copyright Act includes any photograph as well as any building, whether the photograph or building is of artistic quality or not. Similarly, any "compilation in any form", as well as any "computer program", qualifies as a literary work under the Copyright Act, even though such works would not ordinarily be considered a "literary work". It is also noted that apart from "artistic works" and "literary works", the Copyright Act expressly provides for other categories of works such as "musical works", "dramatic works" and "films", which, in the ordinary sense, may also be considered artistic works.

23 Arguably, a broad reading of the Artistic or Literary Exception would also effectively render the News Activity Exception otiose, contrary to the principle of statutory interpretation that an interpretation which does not render a

(*continued on next page*)

21 Nonetheless, whilst the definitions under the Copyright Act cannot be directly imported into the data protection regime, for purposes of determining whether the objective purpose of the work capturing the personal data is for artistic or literary expression, references can be drawn from various judicial considerations as to whether something is art or literature in the context of copyright.

22 In particular, in determining whether something is an artistic or literary work, it is noted that the common judicial approach in the context of copyright is to avoid making judgment on artistic or literary merit. Adopting such an approach would similarly be helpful in the interpretation of the Artistic or Literary Exception under the PDPA. In determining whether the work was created solely for artistic or literary purposes, the focus is not on whether it is good art or bad art. On a related note, the diversity in preferences in relation to artistic and literary expression should be recognised. Art is not just fine art. In determining the range of works to be accepted as having been created for artistic or literary purposes, it should be borne in mind that schools of art and forms of literature are continually being developed.

23 The inherent uncertainty and breadth as to what constitutes art naturally gives rise to difficulties in having a fixed description of its ordinary meaning or scope under the law. The next section of this article discusses further an interesting consideration that has been adopted by various regimes in determining whether something is art – to consider whether or not the work has a functional or utilitarian purpose.

B. Functional or utilitarian purpose

24 In the words of art historian, George Kubler: "We are in the presence of a work of art only when it has no preponderant instrumental use … In short a work of art is as useless as a tool is useful."[24] Whilst the foregoing may sound overly nihilistic, the underlying premise arguably remains

provision otiose is to be preferred to one that does. An in-depth analysis of this point is, however, beyond the scope of this article.

24 Henry Lydiate, "What is Art? A Brief Review of International Judicial Interpretations of Art in the Light of the UK Supreme Court's 2011 Judgment in the Star Wars Case: *Lucasfilm Limited v Ainsworth*" (2011–2013) 4 J Int'l Media & Ent L 111 at 113.

sound, and therefore a helpful guide when determining the applicability of the Artistic or Literary Exception.

25 Such a distinction has underpinned various regimes such as US Custom laws (as briefly touched on above) as well as intellectual property laws, where there is a general policy distinction between useful articles and articles that have "no intrinsic utilitarian function other than to carry the design".[25] Particularly in the US, a "usefulness test" has long been part of its copyright jurisprudence. In *Trans-World Mfg Corp v Al Nyman & Sons, Inc*[26] ("*Nyman*"), in determining whether copyright should be afforded to the design of an eyeglass display case, the US court laid out a definition of a "useful article" as "an article having an intrinsic utilitarian function that is not merely to portray the appearance of the article or to convey information".

26 The usefulness test may be especially helpful in determining the applicability of the Artistic or Literary expression in the context of the PDPA. If an organisation collected the personal data for a "useful article", such as the photograph of any employee in the employer's personnel file on the employee, it cannot be said to have been collected solely for an artistic or literary purpose, as there would be a functional or utilitarian purpose. This approach would appear in line with the legislative intent as articulated by the text of the Artistic or Literary Exception. A profile photograph of the employee, taken by a professional photographer, for the purpose of the business's online portal, annual report, marketing collateral and such will have a mix of both artistic purpose (who does not want to look good in a

---

25 Currently, the Singapore Copyright Act (Cap 63, 2006 Rev Ed) provides for a special exception for artistic works which have been industrially applied, *ie*, the making of a useful article in three dimensions if more than 50 reproductions have been made for purposes of sale or hire (or other qualifying criteria are met). In the Intellectual Property Office of Singapore, *Public Consultation on Proposed Design-Related Legislative Amendments* (11 November 2016) at para 2.2, it was also expressed that: "The designs of useful articles/products, *i.e.* articles/products having an intrinsic utilitarian function other than to carry the design, are more appropriately protected under the registered design regime. However, protection should be via copyright where the article or product has no intrinsic function other than to carry the design."

26 95 FRD 95 (DC Del 1982), referred to in Leonard D DuBoff, "What is Art? Toward a Legal Definition" (1989) 12 Hastings Comm & Ent LJ 303 at 314.

profile photograph?) and a more functional and utilitarian purpose. Nevertheless, in cases where the collection of the photograph by the relevant organisation is for its business's annual report or marketing collateral, *etc*, the collection would ultimately be for a functional purpose. Further, the text of the exception requires that the collection be "*solely* for artistic or literary purposes" [emphasis added], therefore, the Artistic or Literary Exception would unlikely apply should the collection be for a mix of both artistic and functional purposes. It will also be interesting to see how the Artistic or Literary Exception interacts with other concepts in the PDPA (*eg*, deemed consent,[27] the exception for management of employment,[28] *etc*). Consider the inclusion of portraiture photographs like Phan Thi Kim Phuc, the napalm girl in a newspaper or current affairs periodical. Some portraiture photographs are posed (*viz*, there may be express or deemed consent), or taken from across the street in a public place (*viz*, there is the potential application of the Publicly Available Exception). Even if neither exception applies, a portraiture photograph itself may convey information and be incorporated in a newspaper or current affairs periodical as part of an article or its content, and may also come under the News Activity Exception.

27 On a related note, if an individual's employment history was collected by a prospective employer as part of his *curriculum vitae* or if his professional bio profile was collected by a prospective client, such collection would, more likely than not, be for functional purposes.[29] In contrast, the same personal data can be collected solely for conveying the information in a non-fiction book such as a biography or in historical annals, or for adaptation of the information for a historical fiction book. In these circumstances, the works in issue simply add to the pool of knowledge or are to be enjoyed simply from reading them, and have no additional functional purposes. The personal data would therefore have been collected solely for a literary purpose.

---

27 Personal Data Protection Act 2012 (Act 26 of 2012) s 15.

28 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*o*).

29 Other exceptions under the Personal Data Protection Act 2012 (Act 26 of 2012) may apply in such circumstances, such as the exception for work product information in para 1(*n*), and for managing an employment relationship in in para 1(*o*) of the Second Schedule.

28 In the same vein, Stephen McCurry's photograph of the "Afghan Girl" would be solely for an artistic purpose where it is solely to convey the appearance of the portrait. A less straightforward situation is where the personal data captured in the artistic or literary expression are incorporated into another article. Can the personal data still be said to be collected "solely for artistic or literary purposes"? For example, the photographic portrait of the Afghan Girl is placed on the front cover of the *National Geographic* magazine. In this regard, the approach taken by the US Supreme Court in a recent copyright case may guide the determination. In *Star Athletica LLC v Varsity Brands, Inc*,[30] the court held that a "pictorial, graphic or sculptural work" incorporated into a "useful article" is capable of copyright protection if the pictorial, graphic or sculptural features can be identified as a work of art separate from the utilitarian aspects of the article and be capable of existing independently of the utilitarian aspects of the article.

29 A similar approach would likely be persuasive when considering the applicability of the Artistic or Literary Exception under the PDPA. The portrait of the "Afghan Girl" can, for example, clearly be identified as a work of art separate from the rest of the magazine and capable of existing independently of the magazine. It may therefore be argued that the cover of the magazine was to be admired solely for its artistic merit, and therefore the collection of the photograph was solely for artistic purposes.[31] This approach would also appear consistent with the approach taken for UK freedom of information laws, which apply to "information held for purposes other than for journalism, literature or art", in relation to which the UK court opined that any of the BBC's output which did not qualify as journalism would be likely to qualify as literature or as art.[32] In making this

30 Decided on 22 March 2017, available at <www.supremecourt.gov> (accessed 15 May 2017).

31 A similar argument was raised in Leonard D DuBoff, "What is Art? Toward a Legal Definition" (1989) 12 Hastings Comm & Ent LJ 303 at 327–328, albeit in relation to a US Customs case where the court held that the original oil painting by a French painter, which was imported for the purpose of reproducing the painting on the cover of a chemical manufacturer's trade magazine, was for industrial use and not a work of art.

32 See *Sugar v British Broadcasting Corp* [2012] 1 WLR 439; [2012] UKSC 4 at [38].

observation, the UK court appears to have contemplated that different features of the BBC's output, which would likely comprise composite works, can be separately identified as being "journalism", "literature" or "art".

30 Similar concepts abound in Singapore's intellectual property regime. The same definition of a "useful article", as stated by the US courts in *Nyman*, is set out in a statutory exception to copyright under Singapore's Copyright Act.[33] In considering the application of this exception, the Singapore High Court gave an example of a customer wanting a particular picture painted on the top of the car and the manufacturer takes a completed car and spray paints the picture on it. The court opined that the latter act would not be part of the process of "making" a car. Further, the court added that it would not make any difference if the painting was carried out at an earlier stage of the manufacturing process, *eg*, before the wheels are added to the car. In sum, not every act that takes place during the process of manufacture is to be equated with the making of the useful article.[34] Similarly, it may be said that the painting on the car remains solely for artistic purposes.

31 The above should, however, be distinguished from instances where the work of art is collected for purposes of inclusion into a functional or utilitarian work. One such example may be where the art or literary piece is collected as part of the creator's portfolio. In such instances, the collection would more likely be for a functional purpose, rather than solely for artistic or literary purposes.

32 In contrast, there is the UK Supreme Court decision in *Lucasfilm Ltd v Ainsworth*[35] on whether the Imperial Stormtroopers' helmet in the "Star Wars" film was a sculpture for purposes of the UK Copyright, Designs and Patents Act 1988.[36] In this case, the purpose of the helmet was not to appeal as a work of art or to be admired for its appearance. The helmet design was functional in that it was intended to give a particular

33 See Copyright Act (Cap 63, 2006 Rev Ed) s 70 ("Special exception for artistic works which have been industrially applied").

34 *Societe Des Produits Nestlé SA v Petra Foods Ltd* [2014] SGHC 252 at [305].

35 [2012] 1 AC 208.

36 c 48.

impression as part of character portrayal in the film.[37] The UK Supreme Court expressed that: "It was the Star Wars Film that was the work of art that Mr Lucas and his companies created. The helmet was utilitarian in the sense that it was an element in the process of production of the film."[38]

33 In the context of the Artistic or Literary Exception under the PDPA, the collection of personal data for purposes of character portrayal in a film or for inclusion in the biography about the person may arguably be for Artistic or Literary Purposes. That said, as a general matter, it may be helpful to consider whether the collection of personal data in a particular case is actually for a functional purpose that should be distinguished from the eventual artistic or literary work. One such example may be where the names and telephone numbers of the persons interviewed in a documentary film are collected for record purposes. The collection is arguably for a functional purpose rather than for artistic or literary expression, especially since it is part of the functional preparatory work and not used in the final artistic or literary work.

C. Functional, artistic or neither?

34 Admittedly, there can be difficulties in distinguishing whether the work is for an artistic or literary purpose as opposed to a functional purpose, and the difficulties would likely only increase overtime. Carey Young's "Artistic Licence" has already taken a step in this direction.

35 Further, even if it is accepted as a general position that utilitarian works are not artistic or literary works, the converse is clearly not necessarily true. That is, works without a functional purpose are not necessarily artistic or literary works.

36 To aid in the determination, it may be helpful to consider the bases that have been relied on or suggested by the courts of various jurisdictions

---

37 George Wei Sze Shun, *Industrial Design Law in Singapore* (Academy Publishing, 2012) at para 3.54.

38 *Lucasfilm Ltd v Ainsworth* [2012] 1 AC 208 at [44]. Referred to in Henry Lydiate, "What is Art? A Brief Review of International Judicial Interpretations of Art in the Light of the UK Supreme Court's 2011 Judgment in the Star Wars Case: *Lucasfilm Limited v Ainsworth*" (2011–2013) 4 J Int'l Media & Ent L 111 at 142.

that have long been grappling with similar issues. In particular, the following bases have been distilled from several cases (albeit in the context of intellectual property):

> (a) evidence whether the work, or relevant part thereof, is essentially admired or valued simply for the satisfaction, emotional or intellectual, just from looking at it (for an artistic work) or reading it (for a literary work);[39]
>
> (b) whether the work capturing the personal data is displayed in a museum, art gallery, exhibition or sold as a book, *etc*, or otherwise evidence concerning the article's marketability as a work of art or literature;[40]
>
> (c) views from the artistic or literary community including their testimony concerning custom and usage within the art or literary world and the trade in relation to which the article may have a function;[41] and
>
> (d) expert evidence concerning the usefulness of the article or the functional purpose for collecting the personal data.[42]

37 It is noted that the above indicia may also help inform a determination of the subjective intent discussed in Part IV.[43] In sum, it may be assessed holistically, that both the subjective intent as well as objective purpose of the work are for artistic or literary purposes, and in such cases, the Artistic or Literary Exception would apply.

---

39 *George Hensher Ltd v Restawile Upholstery (Lancs) Ltd* [1976] AC 64 in George Wei Sze Shun, *Industrial Design Law in Singapore* (Academy Publishing, 2012) at para 3.51.

40 *Poe v Missing Persons* 745 F 2d 1238 (9th Cir, 1984), referred to in Leonard D DuBoff, "What is Art? Toward a Legal Definition" (1989) 12 Hastings Comm & Ent LJ 303 at 315–316.

41 *Poe v Missing Persons* 745 F 2d 1238 (9th Cir, 1984), referred to in Leonard D DuBoff, "What is Art? Toward a Legal Definition" (1989) 12 Hastings Comm & Ent LJ 303 at 315–316.

42 *Poe v Missing Persons* 745 F 2d 1238 (9th Cir, 1984), referred to in Leonard D DuBoff, "What is Art? Toward a Legal Definition" (1989) 12 Hastings Comm & Ent LJ 303 at 315–316.

43 See paras 16–18 above.

VI. Concluding thoughts

38 In the face of innovative art forms and practices that challenge traditional concepts of art and literature, there is undoubtedly increasing difficulty in determining whether something is "solely for artistic or literary purposes". Notwithstanding the difficulties in delineating the boundaries of the exception, the Artistic or Literary Exception plays an important role in the overall scheme of the PDPA. As a general matter, artists should not be restrained from painting portraits of individuals and writers should not be prevented from writing biographies. As creators continue to push the boundaries of what is presently accepted as art and literature, it is foreseeable that the balance to be struck between data protection and freedom of expression is a dynamic one and the right balance will depend on the facts in individual cases. In this regard, it is worth noting that the PDPA requires organisations to collect, use and disclose personal data only for purposes that a reasonable person would consider appropriate.[44] Inherent in this requirement are considerations of proportionality which would help ensure that any collection, use or disclosure of personal data without consent pursuant to the Artistic or Literary Exception is not disproportionate to the artistic or literary purpose being contemplated. Further, the PDPA makes it clear that it does not affect any existing obligations under other laws,[45] and other laws such as the tort of defamation or confidentiality will also serve to act as a balance against the Artistic or Literary Exception.

---

44 Personal Data Protection Act 2012 (Act 26 of 2012) s 18.

45 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(6).

PROTECTING THE RIGHT OF PUBLICITY UNDER THE PERSONAL DATA PROTECTION ACT*

Gilbert LEONG†
LLB (National University of Singapore),
LLM (University College London)

FOO Maw Jiun‡
LLB (National University of Singapore)

Kenneth FOK§
LLB (National University of Singapore)

I. Introduction

1 In Singapore, there is no clear legal recognition of the right of publicity (also known as "personality rights" in some jurisdictions). However, with the coming into force of the Personal Data Protection Act 2012[1] ("PDPA"), it may be said that information pertaining to identity now enjoys a considerable degree of statutory protection.

2 Given that there is some overlap between the PDPA and the right of publicity in terms of the nature of the information that they protect, this article seeks to explore whether the provisions of the PDPA can be relied upon to effectively create a right of publicity regime in Singapore.

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Senior Partner, Dentons Rodyk & Davidson LLP, IP & Technology Practice Group. Gilbert is very active in the field of data privacy/protection matters, having acted for large financial institutions, healthcare providers and industrial companies. He has also written and spoken widely on the area.

‡ Partner, Dentons Rodyk & Davidson LLP, IP & Technology Practice Group.

§ Associate, Dentons Rodyk & Davidson LLP, IP & Technology Practice Group.

1 Act 26 of 2012.

II. What is the right of publicity?

3 The right of publicity can be broadly understood as *the right of an individual to control how his identity is commercially used*. In the seminal case of *Haelen Laboratories v Topps Chewing Gum, Inc*[2] ("*Haelen*"), the US Court of Appeals for the Second Circuit explained as follows:

> We think that, in addition to and independent of that right of privacy (which in New York derives from statute), a man has a right in the publicity value of his photograph, *ie*, the right to grant the exclusive privilege of publishing his picture, and that such a grant may validly be made 'in gross,' *ie*, without an accompanying transfer of a business or of anything else. Whether it be labelled a 'property' right is immaterial; for here, as often elsewhere, the tag 'property' simply symbolizes the fact that courts enforce a claim which has pecuniary worth.
>
> This right might be called a 'right of publicity.' For it is common knowledge that many prominent persons (especially actors and ball-players), far from having their feelings bruised through public exposure of their likenesses, would feel sorely deprived if they no longer received money for authorizing advertisements, popularizing their countenances, displayed in newspapers, magazines, busses, trains and subways.

4 In the years since *Haelen*, the right of publicity has received protection in the US under the Lanham Act at the federal level, and through various statutes and common law regimes at the state level. Notably, however, the manner and degree to which the right of publicity is protected in the US (and whether the right of publicity is protected at all) varies between different states, and also between federal and state laws.

5 Beyond the US, there is also a significant degree of variance in protection for the right of publicity. For example, in the UK, there is no explicit right of publicity at all. Therefore, parties seeking to protect their personality rights in the UK have had to rely on alternative legal routes such as the laws on passing off, misuse of private information and breach of confidence.

6 Given that the right of publicity is treated differently in different jurisdictions, it is difficult – if not altogether impossible – to provide a singular and definitive pronouncement what this right specifically entails.

---

2 202 F 2d 866 at 868 (2nd Cir, 1953).

As such, for the sake of clarity, this article will use California's right of publicity regime as the standard to which the PDPA will be compared.

7 In California, the right of publicity is protected under both statute and common law. Section 3344(a) of the California Civil Code states as follows:

> Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent … shall be liable for any damages sustained by the person or persons injured as a result thereof …

8 California's common law regime was articulated in *Eastwood v Superior Court*,[3] where the California Court of Appeal described the elements of the tort of "commercial appropriation of the right of publicity" as

> (1) the defendant's use of the plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, …; (3) lack of consent; and (4) resulting injury.

9 In contrast to California, and like the UK, Singapore has no explicit right of publicity. Consequently, parties seeking to protect their personality rights in Singapore have also had to rely on alternative causes of action.

10 For example, in *Chiam See Tong v Xin Zhang Jiang Restaurant Pte Ltd*[4] ("*Chiam*"), the plaintiff's photograph had been used in business promotional materials without his consent. For what was effectively a breach of his right of publicity, the plaintiff sued under the tort of defamation.

11 The Singapore High Court found in favour of the plaintiff and held that the use of the photograph by the defendant was defamatory because it suggested that the plaintiff had consented to the use of his photograph for publicity "either for gain or to sponsor a private restaurant and that [the plaintiff] had done so by taking advantage of his position as a Member of Parliament and also for the benefit of promoting himself as an advocate and

3 149 Cal App 2d 409 (Cal Ct App, 1983).

4 [1995] 1 SLR(R) 856.

solicitor".[5] The judge added that "[i]n my view, a substantial proportion of the responsible and right-thinking English but non-Chinese readership would have thought less well of the plaintiff after reading the handbills".[6]

III. Relevant sections of the Personal Data Protection Act

12 Turning now to the PDPA, it can be generally stated that the PDPA aims to "[regulate] the proper management of personal data" so as to "safeguard individuals' personal data against misuse".[7] Under the PDPA, *organisations* are subject to wide-ranging restrictions and obligations in relation to how they may, among other things, collect, use, disclose, retain and transfer personal data.

13 For the purposes of investigating the extent to which the PDPA may overlap with the right of publicity, the following provisions of the PDPA are relevant:

> (a) **Section 13 of the PDPA**. This section stipulates that organisations are not allowed to collect, use or disclose personal data about an individual unless the individual gives, or is deemed (see s 15 of the PDPA on "deemed consent") to have given, his consent for such collection, use or disclosure.
>
> (b) **Sections 18 and 20 of the PDPA**. Under s 18 of the PDPA, an organisation may only collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances. This is coupled with s 20 of the PDPA, under which the organisation must inform the individual what those purposes might be before collecting his personal data.
>
> (c) **Section 32 of the PDPA**. This section provides that any person who suffers loss or damage as a result of a breach of ss 13, 18 and 20 of the PDPA has a right of action for relief in civil proceedings

5 *Chiam See Tong v Xin Zhang Jiang Restaurant Pte Ltd* [1995] 1 SLR(R) 856 at [7].

6 *Chiam See Tong v Xin Zhang Jiang Restaurant Pte Ltd* [1995] 1 SLR(R) 856 at [7].

7 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

and may be entitled to remedies including relief by way of injunction or declaration and damages.

14 It is critical to note that the term "personal data" is defined in s 2 of the *PDPA* as "data, whether true or not, about an individual who can be identified — (*a*) from that data; or (*b*) from that data and other information to which the organisation has or is likely to have access". Pertinently, the above definition does not place a limit on the types of information that can count as personal data. Therefore, when interpreted broadly, it is conceivable that any form of data concerning an individual could count as personal data. As the Personal Data Protection Commission's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[8] ("PDPC Guidelines") explain, examples of personal data include an individual's full name, passport number, telephone number, thumbprint, and *photographs, videos or other images* of that individual.[9]

IV. Could the Personal Data Protection Act be used to enforce a right of publicity in Singapore?

15 Having briefly explored the right of publicity and the PDPA in the paragraphs above, it should be apparent that the two doctrines have interesting areas of overlap. For example, under the above-mentioned definition of "personal data", it is possible for many aspects of a person's "identity" or "image" to be protected by the PDPA. Consequently, similar to enforcing his right of publicity, an individual whose image has been used without his consent may be able to rely on the PDPA to stop such use, and also to possibly recover damages.

16 In fact, one could argue that the PDPA offers even more protection for identity-related information than the right of publicity. For example:

(a) The PDPA may protect a *wider range* of information than the right of publicity. As stated above, the right of publicity protects "the plaintiff's identity", which can include his name, voice, signature, photograph or likeness. Notably, in *White v Samsung Electronics*

8 Revised on 15 July 2016.

9 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at p 14.

America, Inc[10] ("*White v Samsung*"), the US Court of Appeals for the Ninth Circuit held that the range of information protected under the right of publicity extends beyond the traditional categories such as name and likeness, and includes *any element* (or combination of elements) that can evoke the plaintiff's personality (such as voices, gestures and roles).

In comparison, it is arguable that the PDPA goes even further in terms of the scope of the information that it protects. First off, protection under the PDPA is not limited by any need to *"evoke" a person's identity*. Under the PDPA, protection is available as long as there is information from which an individual *can be identified*. It is argued here that there is a nuanced but important difference between "information that can evoke an identity" and "information that can identify a person". The former pertains only to information that can bring a person's identity to mind, whereas the latter can include any information that can be used to find out who a person is. As such, the latter is likely to have a far broader ambit. For example, types of information such as telephone numbers and passport numbers are unlikely to evoke a person's identity; but can be used to identify a person. In such scenarios, protection would be available under the PDPA, but not the right of publicity. On the flipside, it is likely that almost every form of information that can evoke a person's identity could also be used to identify a person. This nuanced dichotomy reflects the fact that the two legal concepts are actually rather different in nature. As mentioned above, the right of publicity is meant to protect the commercial value of a person's public identity. In contrast, the PDPA is meant to protect information about a person.

Secondly, it is important to remember that "personal data" is defined such that the PDPA even protects information that, *when used with other information*, can identify a person. Therefore, even pieces of information that cannot *independently* identify a person (or evoke a person's identity) can be protected by the PDPA as long as they are accompanied by other appropriate bits of information. This is another reason why the PDPA may provide even more protection than the right of publicity.

10 971 F 2d 1395 at 1399 (9th Cir, 1992).

(b) Furthermore, the PDPA offers two distinct avenues of enforcement. First, an aggrieved party can rely on regulatory enforcement by lodging a complaint with the Personal Data Protection Commission ("PDPC"), which can then conduct investigations and make directions to ensure compliance. Second, there is the option of a private action under s 32 of the PDPA, which allows an aggrieved party who has suffered loss or damage resulting from a breach of the PDPA to seek relief in civil proceedings.[11]

A. Limitations of the Personal Data Protection Act

17 However, on closer scrutiny, the PDPA actually offers less protection than the right of publicity.

(a) The most significant limitation is that the PDPA does not protect data that is publicly available.[12] Section 2(1) of the PDPA defines "publicly available" personal data to be:

> … personal data that is *generally available to the public*, and includes personal data which *can be observed by reasonably expected means at a location or an event* —
>
> (a) *at which the individual appears; and*
>
> (b) *that is open to the public*.
>
> [emphasis added]

The closest judicial pronouncement of what it means to be "generally available to the public" is how the Singapore courts have approached the question of what is "freely available in the public domain" in confidentiality cases. In short, whether any piece of personal data can be considered publicly available personal data would entail an assessment taking into consideration factors affecting the extent of accessibility of the information to members of the general public. The PDPC Guidelines add that "[p]ersonal data is generally available to

11 Unlike the Californian common law action protecting the right of publicity, the Personal Data Protection Act 2012 (Act 26 of 2012) does not require the appropriation of the personal data to be for the defendant's advantage.

12 Section 17 of the Personal Data Protection Act 2012 (Act 26 of 2012) read with the Second, Third and Fourth Schedules.

the public if any member of the public could obtain or access the data with few or no restrictions".[13]

Next, the term "publicly available" also includes "personal data which can be observed by reasonably expected means at a location or an event at which the individual appears; and that is open to the public". As explained in the PDPC Guidelines, it is an objective question of whether or not "individuals *ought to reasonably expect* their personal data to be collected in that particular manner at that location or event"[14] [emphasis added]. The PDPC Guidelines go on to explain "open to the public" as follows:[15]

> A location or event would be considered 'open to the public' if members of the public can enter or access the location with few or no restrictions. Generally speaking, the more restrictions there are for access to a particular location, the less likely it would be considered 'open to the public'. Relevant considerations would be factors that affect the ease and ability with which the public can gain access to the place. Examples include the presence or absence of physical barriers, such as fences, walls and gates, around the place; the conditions and effectiveness of these barriers; and the employment of security systems, sentries and patrols aimed at restricting entry.

The "publicly available" exception reflects the fact that unlike the right of publicity, the PDPA does not confer property rights over a person's identity. Instead, the PDPA only seeks to protect his right to privacy in relation to his personal data.

Consequently, if the photograph containing the image of an individual is already publicly available, or if the photograph was taken of the individual at a location or event that was open to the public, recourse under the PDPA will be limited, even if that image was used without his consent. In this way, the scope of protection granted by the PDPA pales in comparison to protection under the right of publicity.

---

13 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at p 54.

14 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at p 56.

15 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at p 56.

(b) Furthermore, the PDPA does not apply to individuals acting in their personal or domestic capacities.[16] Granted that breaches of the right of publicity are often perpetuated by commercially-driven organisations, this limitation effectively means that an individual who has his identity or image misused or exploited by an individual (acting in his personal capacity) would not be able to take any action under the PDPA, which action would otherwise be permitted if one were to rely on the right of publicity.

(c) Finally, as stated above, the scope of the right of publicity in California post-*White v Samsung* has been expanded to include any element (or combination of elements) that can evoke the plaintiff's personality such as voices, gestures and roles (think the distinctive voices of Morgan Freeman, James Earl Jones or Winston Churchill, or the roll of Rowan Atkinson's eyeballs). In other words, if a person is known by a unique feature such as a role that he has played, or by a gesture that he frequently makes, then the right of publicity would protect that famous role or gesture. In contrast, it is uncertain whether the PDPA will protect such unique forms of information. Nevertheless, bearing in mind that the PDPA does not strictly limit the forms and manifestations of information that count as "personal data", the possibility of such unique forms of information being protected cannot be ruled out altogether.

18 With the foregoing paragraphs in mind, it is not inconceivable that the PDPA may be used as a makeshift right of publicity. However, a plaintiff who seeks to use the PDPA in this way is likely to find that the efficacy of such an approach predicates upon the circumstances of his case, and the specific outcomes sought by him. In addition, as discussed below, using the PDPA as a makeshift right of publicity may not always be a good idea.

V. Concluding thoughts

19 Even if the PDPA can be used to protect the right of publicity, there are several reasons why this *may not be advisable*.

20 First, there does not appear to be any legislative basis for using the PDPA as a makeshift right of publicity. Fundamentally, the PDPA is meant

16 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(1).

to protect individuals' personal data, and not to create proprietary rights in such data. As explained in Parliament by Dr Yaacob Ibrahim, the PDPA is "a data protection regime [that] is necessary *to address individuals' growing concerns over the use of their personal data and to maintain individuals' trust in organisations that manage data*"[17] [emphasis added]. This rationale is also reflected in s 3 of the PDPA, which provides that the "purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the *right of individuals to protect their personal data* and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances" [emphasis added]. Therefore, using the PDPA as a "back door" to enforcing the right of publicity pushes it into a realm that may not have been contemplated or intended by the Legislature at all.

21 Second, using the PDPA as a makeshift right of publicity comes at the risk of overlooking competing rights and interests. In many jurisdictions, the right of publicity is balanced against (and circumscribed by) competing interests such as the freedom of speech and expression. For example, in the US, the right of publicity is limited by the First Amendment (which provides constitutional protection for the right to free speech). In the UK and the European Union, such freedoms also function as counterbalances to privacy or publicity rights. The tension between competing rights plays an important and perceptible role in preventing the overexpansion of the right of publicity. For instance, US courts have generally allowed the right of publicity to apply with more force in relation to speech that is commercial in nature, and less so in relation to speech that is expressive or artistic in nature.

22 In the case of the PDPA, less attention may have been paid to balancing competing interests since the PDPA was not meant to protect publicity rights in the first place. While the PDPA does have its own set of limitations as enumerated in its Second and Third Schedules,[18] these

17 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

18 There are provisions in the Second and Third Schedules to the Personal Data Protection Act 2012 (Act 26 of 2012) which prescribe the circumstances where personal data can be collected and used without consent. These

(*continued on next page*)

limitations were not drafted with publicity rights in mind and therefore may not be sufficient. It is also noteworthy that while Art 14 of the Constitution of the Republic of Singapore[19] provides for the freedom of speech and expression, this freedom is available only to "citizens of Singapore" and is unlikely to be available to the "organisations" that are subject to the PDPA. Hence, using the PDPA as a right of publicity runs the risk of creating an overly draconian regime that runs roughshod over other interests.

23 Third, it seems that an individual's prominence or public image would instead work against him if he were to rely on the PDPA to seek redress against a breach of his right of publicity. With the PDPA's exception for "publicly available information", a truly "private" individual whose right of publicity is breached would arguably stand a better chance of relying on the PDPA to seek redress. In the case of *Chiam*, the plaintiff was a prominent politician, a Member of Parliament and an advocate and solicitor, and that was why he succeeded in bringing a case for defamation for what was essentially a breach of his right of publicity. It is probably unlikely that other individuals who are not public figures or do not enjoy a certain standing in society would have succeeded in such a case if their identity or image had been misused.

24 There is yet to be any jurisprudence on s 32 of the PDPA and it remains to be seen how the Singapore courts might approach a private action taken by an individual to effectively protect his right of publicity through the PDPA. It is hoped that if and when such an opportunity arises, the issues arising from this article will be adequately considered and addressed.

---

circumstances include those which are commonly considered in the balance for right of publicity cases, including where the collection and use is necessary in the national interest; where the personal data is used for a research purpose, including historical or statistical research; where collection and use of personal data is solely for artistic or literary purposes; and where collection and use of personal data is for news activity.

19 1999 Rev Ed.

DATA PROTECTION OFFICER'S ROLE IN ACCOUNTABILITY*

Lanx GOH†
LLB (University of Birmingham), DipSing (National University of Singapore), LLM (University of California, Berkeley), MSc (University of Oxford); CIPM, CIPP/A/E, FIP; Advocate and Solicitor (Singapore); Accredited Mediator (Singapore International Mediation Institute)

I. Introduction

1 The data protection provisions of the Singapore Personal Data Protection Act[1] ("PDPA") came into effect on 2 July 2014. Since then, the Singapore Personal Data Protection Commission ("PDPC")[2] has taken 26 organisations[3] and one registered salesperson[4] to task.[5] That said, one needs to bear in mind that the objective of the PDPA is not to *discourage* the use of personal data, but to balance the interests of businesses and

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors remain the author's own.

† Team Lead, Investigations Unit (Data Protection and Do Not Call), Personal Data Protection Commission; Fellow of Information Privacy (International Association of Privacy Professionals).

1 Act 26 of 2012.

2 The Singapore data protection authority.

3 From 2 July 2014 to 31 March 2017.

4 Organisations were found in breach of various provisions of the Personal Data Protection Act (Act 26 of 2012) ranging from the protection obligation under s 24 to the consent and notification obligations under ss 13 and 20. See the Personal Data Protection Commission's website for the Commission's enforcement decisions <https://www.pdpc.gov.sg/commissions-decisions/data-protection-enforcement-cases>. See also Irene Tham, "Time to Step Up Efforts to Ensure Security of Personal Information" *The Straits Times* (1 February 2017).

5 The merits of which will not be discussed in this article due to conflict of interests and confidentiality issues. That said, it is noteworthy that the Personal Data Protection Commission has been one of the most active and efficient data protection authorities in enforcing its data protection law.

consumers.[6] Singapore understands that "[a] [general] data protection regime to govern the collection, use and disclosure of personal data is necessary to address individuals' growing concerns over the use of their personal data and *to maintain individuals' trust* in organisations that manage data" [emphasis added] in today's society where business use of personal data is growing "exponentially as infocomm technologies like high-speed computing and business analytics enable the processing of large amounts of personal data".[7] The aforesaid will enhance Singapore's competitiveness and strengthen its position *as a trusted business and global data hub*.[8] In this regard, the Executive Chairman of the Data Protection Advisory Committee,[9] Leong Keng Thai,[10] commented: "[P]ersonal data, is essential to innovation in today's economy … use the information for business competitiveness, but use it responsibly, and take appropriate measures to protect personal data."[11] Minister for Communications and Information, Dr Yaacoob Ibrahim, reiterated the same point:[12] "Data is the 'new oil' of the 21st Century … the collection and the use of data must rest upon *a foundation of trust*." [emphasis added]

---

6 See s 3 of the Personal Data Protection Act (Act 26 of 2012) and Simon Chesterman, "From Privacy to Data Protection" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2014) at p 23.

7 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

8 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

9 The Data Protection Advisory Committee has been appointed under the Personal Data Protection Act (Act 26 of 2012) to advise the Personal Data Protection Commission on matters relating to the review and administration of the personal data protection framework.

10 Leong Keng Thai was formerly the Chairman of the Personal Data Protection Commission.

11 Irene Tham, "Singapore Privacy Watchdog Fines and Warns 11 Organisations for Data Breaches" *The Straits Times* (21 April 2016).

12 Dr Yaacob Ibrahim, Minister for Communications and Information, speech at the opening of the Fourth Personal Data Protection Seminar (20 July 2016).

2 The above shows that the creation of trust between consumers and businesses is the key enabler for the use of personal data, and therefore enhancement of Singapore's competitiveness.[13] The 2016 consumer survey on the PDPA conducted by the PDPC indicates that 91.6% out of 1,502 interviewed individuals feel that the PDPA has been effective in protecting their personal data.[14] This evinces the high level of confidence that consumers in Singapore have in the PDPA and the likelihood of them allowing organisations to collect, use and disclose their personal data. However, with the rapid advancement of technology such as cloud computing and the fact that most published breaches in Singapore involved small and medium-sized enterprises ("SMEs"), it is worthwhile to examine how an efficient and competent data protection law like the PDPA can be further developed to improve the confidence that consumers have in the law, and the environment of trust between businesses and consumers, and establish a protected and consented flow of personal data for commercial use in today's globalised and digital economy.

3 On this subject, the answer is the concept of accountability. In recent years, accountability has become the pillar of effective data protection and a prevalent trend in global data privacy law.[15] Privacy Commissioner for Hong Kong, Stephen Wong, opined that the emphasis in data protection should shift from compliance to accountability,[16] in that organisations ought to view privacy[17] not as a liability but an asset. If organisations embrace data protection through privacy management programmes ("PMP"), privacy by design and default ("PBDD") and so on, they can gain consumers' trust, demonstrate privacy compliance to the data protection authority ("DPA"), and increase competitiveness as a result. The

13 See *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

14 See https://www.pdpc.gov.sg/docs/default-source/Reports/consumer-survey-2016---infographics-v2.pdf?sfvrsn=0 (accessed 2 May 2017).

15 Bojana Bellamy, "The Rise of Accountability from Policy to Practice and Into the Cloud" (International Association of Privacy Professionals, 10 December 2014).

16 Sam Pfeifle, "Meet Hong Kong's New DPA" (International Association of Privacy Professionals, 25 August 2015).

17 The terms privacy and data protection will be used interchangeably even though the author acknowledges the differences between the two.

importance of accountability is evident. Besides being the key concept underlying the European Union ("EU") General Data Protection Regulation[18] ("GDPR"),[19] it has been implemented via ISO 27018 data privacy cloud standard as a tool to guide cloud service providers in terms of privacy and security requirements.[20]

4 Then how should Singapore improve accountability under its existing PDPA regime? The solution is through enhancing the capability and role of data protection officers ("DPO"). According to the Data Protection Working Party established by Art 29 of EU Directive 95/46/EC ("Article 29 Data Protection Working Party"), the DPO is the cornerstone of accountability and appointing a DPO can facilitate compliance[21] that is necessary to build trust and business competitiveness. That said, the accountability among Singapore organisations can only be improved if DPOs possess the right level of data protection expertise and knowledge. This article will explore the current requirement for DPOs under the PDPA, whether Singapore will pursue the professionalisation of DPOs in the future, what benefits will ensue, and the requirements, obligations and power of DPOs.[22] In this vein, it is logical to examine the possibility of professionalising DPOs in Singapore by making reference to the GDPR which provides detailed DPO obligations and requirements with accountability as the lynchpin.

18 Regulation (EU) 2016/679.

19 The General Data Protection Regulation (Regulation (EU) 2016/679) is due to replace Directive 95/46/EC on 25 May 2018.

20 Bojana Bellamy, "The Rise of Accountability from Policy to Practice and Into the Cloud" (International Association of Privacy Professionals, 10 December 2014).

21 Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers" (WP 243) (13 December 2016) at p 4.

22 This article does not attempt to provide an overview of the Personal Data Protection Act (Act 26 of 2012), nor address all its possible gaps and possible reforms.

II. Data protection officer

5 Data is the new currency especially in view of a globalised economy driven by concepts such as big data,[23] cloud technology[24] and the Internet of Things.[25] Organisations now process[26] large amounts of personal data on a daily basis for commercial needs, and the processing activity and amount are only likely to increase in the future in Singapore with its Smart Nation initiative and aspiration to be a global business and data hub. As such, it is essential to have professional DPOs to ensure accountability is embedded in the practices and policies of every organisation that processes personal data in Singapore.

A. Under the Personal Data Protection Act

6 Section 11(3) of the PDPA states an organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA.[27] Group companies can appoint a single DPO provided that he is easily accessible from each establishment as a DPO is

23 Big data is information characterised by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value. See Andrea De Mauro, Marco Greco & Michele Grimaldi, "A Formal Definition of Big Data Based on Its Essential Features" (2016) 65(3) *Library Review* 122.

24 Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*eg*, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. See Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing* (National Institute of Standards and Technology, 2011) Special Publication 800-145.

25 The Internet of Things is the infrastructure of the information society that enables advanced services through interconnecting devices, which then serves as a catalyst for a greater flow of information. See International Telecommunication Union, "Overview of the Internet of Things" (2012).

26 See s 2 of the Personal Data Protection Act (Act 26 of 2012) for the definition of "processing".

27 Sections 11(3) and 12 of the Personal Data Protection Act (Act 26 of 2012) require all organisations in Singapore that handle personal data to have a data protection officer and privacy policy to ensure compliance with the Act.

also the contact point with respect to data subjects and DPAs, and internally for each company. A DPO can be a member of staff or a hired contractor.[28] It is economically sensible to allow group companies to appoint a single DPO (with required expertise and knowledge), or outsource the appointment as both can reduce costs for the group companies. The latter can also aid in professionalising and industrialising DPOs with companies providing professional DPO services. Under the current PDPA,[29] organisations are permitted to hire external DPOs and to share DPOs between group companies. The aforesaid has been confirmed by the PDPC's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*.[30]

7 A related provision is s 12 of the PDPA, which requires an organisation to put in place policies and practices to meet its obligations under the PDPA. The correlation between ss 11(3) and 12 is policies and practices are only as effective as the person devising and implementing them. The knowledge and expertise of the person that is designated is therefore pivotal to the successful implementation of data protection policies and practices to ensure PDPA compliance.[31] For example, a DPO who has years of experience in data protection and has obtained qualifications such as Certified Information Privacy Manager ("CIPM") and Certificated Information Privacy Professional ("CIPP")[32] would be able to devise comprehensive PMP or incorporate PBDD into the infrastructure and products of the organisation.

---

28 Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers" (WP 243) (13 December 2016) at pp 10 and 12.

29 Section 11(3) of the Personal Data Protection Act (Act 26 of 2012).

30 Revised on 15 July 2016. See para 17.2.

31 Hannah Lim Yee Fen, "Data Protection in the Employment Setting" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2014) at p 113.

32 "Certified Information Privacy Manager" and "Certificated Information Privacy Professional" are specialised certificates issued by the International Association of Privacy Professionals which relate to data protection and privacy operations, laws, regulations and framework. There are many other certificates issued by other data protection and privacy associations like the Law Society of Ireland and PDP Training.

8 It is noted that s 11(3) does not compel organisations to appoint a professional DPO, *ie*, the expertise required from the DPO is not defined. The appointed person should possess *reasonable*[33] expertise and knowledge to advise the organisation on PDPA compliance in the context of the organisation's business. Some organisations in Singapore comply with the requirement under s 11(3) by designating a human resource officer or any available staff to be the DPO, who in most cases may not be trained in data protection related matters nor well versed in the PDPA.[34] This is particularly true for SMEs where cost and manpower constraints are a concern. However, the author has also encountered many SME DPOs who are trained in data protection. This is due to the relentless effort of the PDPC in providing affordable PDPA training and reaching out to the various stakeholders via the Fundamentals of the Personal Data Protection Act ("Fundamentals PDPA") course,[35] outreach efforts and its seven training partners like the Singapore Academy of Law.[36] Likewise, larger SMEs or multinational companies will usually engage a professional DPO, or at least appoint their compliance officer or in-house counsel as the DPO.

9 An examination of some of the enforcement actions taken by the PDPC shows organisations found in breach of the PDPA could have avoided the outcome if they had employed a professional DPO. For example, K Box Entertainment Group Pte Ltd ("K Box"), which received the highest financial penalty of $50,000, did not have a DPO at the material time and was directed by the PDPC to appoint one. K Box was also found to be in breach of the protection obligation under s 24 of the PDPA where weaknesses in relation to its access control (*eg*, weak password policy), weak control over unused accounts, and failure to conduct audits of

33 Section 11(1) of the Personal Data Protection Act (Act 26 of 2012) states: "In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances."

34 Hannah Lim Yee Fen, "Data Protection in the Employment Setting" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2014) at p 112.

35 Developed under the Business Management Workforce Skills Qualifications (BM WSQ) framework.

36 For details of the course and all seven training providers, see the Personal Data Protection Commission's website https://www.pdpc.gov.sg/organisations/data-protection-officers.

its security system presumably led to the data breach incident involving disclosure of more than 350,000 members' personal data.[37] The weaknesses or lapses identified in the K Box case are not sophisticated problems. If K Box had employed a professional DPO who had then conducted a data protection impact assessment ("DPIA") when the PDPA came into effect, the aforesaid problems would have been detected and fixed.

B. Possibility of professionalising data protection officers in Singapore

10 At the International Association of Privacy Professionals ("IAPP") Asia Privacy Forum 2016, the Deputy Commissioner of the PDPC, Yeong Zee Kin,[38] remarked that the PDPC is looking to professionalising DPOs as a career in Singapore to improve compliance with the PDPA. Indeed, the PDPC has recently awarded a DPO certification project[39] that aims to provide advanced DPO training which serves as a continuation of the Fundamentals PDPA course mentioned above.[40] Besides the certification project, there has been market talk among stakeholders and DPOs about the creation of a Singapore DPO association. A DPO association, if formed, will aid the professionalisation of DPOs immensely. For example, in Hong Kong, the Data Protection Officers' Club[41] provides DPOs with a platform for advancing knowledge, sharing experience and

37 See *K Box Entertainment Group Pte Ltd and Finantech Holding Pte Ltd* [2016] SGPDPC 1.

38 Formerly known as Commission Member of the Personal Data Protection Commission.

39 Among the Personal Data Protection Commission's many other initiatives to help organisations to comply with the Personal Data Protection Act (Act 26 of 2012).

40 In relation to specific training as to the Personal Data Protection Act (Act 26 of 2012) for data protection officers, there are the CIPP/Asia and Hands-on Data Protection Officer Training Programme offered by the International Association of Privacy Professionals and Straits Interactive Pte Ltd respectively.

41 The Data Protection Officers' Club was formed in 2010 and currently has a membership of 539 members (as of March 2016). See Stephen Kai-yi Wong, Privacy Commissioner for Personal Data Hong Kong, China, "Hong Kong Personal Data Protection Regulatory Framework: An Approach to Consultative Regulation", speech delivered at the IAPP Global Privacy Summit 2016 (6 April 2016).

providing continuous data protection training. Like for any other professionals such as doctors or lawyers, in addition to the legal requirements, an association helps to maintain the standard and capability of its industry. Judging from these moves, the professionalisation of DPOs in Singapore could very well take place in the future.

C. Benefits of professionalising data protection officers in Singapore

11 The key benefit of professionalising DPOs is the improved accountability among organisations processing personal data in Singapore. The appointment of a DPO is critical towards accountability as, ultimately, he will be responsible for ensuring accountability in the organisation's policies and practices, and demonstrating compliance to the DPA through proper documentation, data governance, data inventory, PMP, PBDD and DPIA. However, this is not achievable if the DPO does not possess the relevant expertise and knowledge. As Singapore transforms itself into a Smart Nation, a more robust personal data protection regime is needed to safeguard the enormous amount of private information generated by high-tech Internet-enabled gadgets.[42] In this aspect, professional DPOs, especially those with technical expertise, are essential for organisations using technology in their business. For example, PBDD and DPIA may be imperative for organisations that sell Internet-enabled gadgets or conduct online sales that will involve large scale processing of personal data.

12 Another benefit is job creation. At the IAPP Asia Privacy Forum 2016, the IAPP President and CEO, Trevor Hughes, pointed out that the GDPR has made the provision of a DPO mandatory for certain companies. This professionalises the career, creates 28,000 new jobs and reduces data breach in the EU. IAPP has recently revised the number of new jobs to 75,000 worldwide from the earlier projected figure of 28,000 as the GDPR regulates the privacy practices of any company handling EU citizens' data, whether or not that company is located in the EU. This estimate includes 715 professional DPOs from Singapore as it is one of the

42 Tan Teck Boon, "In Smart Nation drive, S'pore must strengthen personal data protection" *The Straits Times* (2 March 2016).

EU's common trading partners.[43] The author is of the opinion that the GDPR will not only create jobs, but lead to the "professionalisation" and "industrialisation" of DPOs. The former is about enhancing the knowledge and capability of DPOs and making it a professional career to attract talented individuals to join the industry, whereas the latter is to create external DPOs that concurrently serve many SMEs that do not have the right person internally to do the job, or find it too costly to hire a professional DPO.[44] Either way, jobs will be created if Singapore professionalises and/or industrialises its DPOs.

D. Requirements, obligations and power of data protection officers

13 As discussed above, all organisations in Singapore that handle personal data are required to appoint a DPO for ensuring compliance with the PDPA,[45] Singapore is moving towards professionalising DPOs and there are clear benefits from doing so. The fundamental question is what the requirements, obligations and power of DPOs are. Notwithstanding s 11(3) does not prescribe the aforesaid in detail, they should be determined based on what a reasonable person would consider appropriate in the circumstances under s 11(1) of the PDPA. A "reasonable person" is judged based on an objective standard and is evolutionary.[46] Since accountability is a key concept that underpins the GDPR, it is useful to make reference to the EU legislation while determining what requirements, obligations and power a reasonable person would expect DPOs to have in order to instil accountability into the culture, policies and practices of organisations.

---

43 Rita Heimes & Sam Pfeifle, "Study: GDPR's global reach to require at least 75,000 DPOS worldwide" (International Association of Privacy Professionals, 9 November 2016).

44 David Meyer, "How to 'Industrialize' the Data Protection Officer Role?" (International Association of Privacy Professionals, 23 August 2016). Some organisations like Rajah & Tann Singapore LLP are offering full-fledged data protection officer services in Singapore. See also Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers'" (WP 243) (13 December 2016) at p 12.

45 Personal Data Protection Act (Act 26 of 2012) s 11(3).

46 See para 9 of Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016).

(1) Requirements

15 In relation to the precise requirements expected from a DPO, it is convincing and logical to conclude that a reasonable person would consider the nature of the data processing activity of an organisation in determining them, that is, the larger the volume or the more sensitive the personal data processed by an organisation, the higher the qualities and knowledge the DPO should possess.[47] The aforesaid finds support from the GDPR. First, under Art 37 of the GDPR, it is now mandatory for organisations (both data controllers and processors) to have a DPO when their core activities require regular, systematic and large scale[48] monitoring of data subjects or large scale processing of sensitive data. Core activities include activities where the processing of data forms an inextricable part of the organisation's activities, like hospitals cannot provide healthcare services without processing health data. However, it does not encompass ancillary activities like paying employees.[49] This means healthcare related companies, technology companies (especially those performing tracking and profiling on the Internet like Google) and biotech companies[50] must appoint

47 See Table 11 and para 14.3 of Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* (revised on 20 January 2017) and para 25.2.5 of Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (21 April 2016). The former recommends encryption of sensitive data that has a higher risk of adverse impact to individuals as good practice, and the latter explicitly states that failure to put in place safeguards proportional to the harm that might be caused by disclosure of that personal data when an organisation is handling a large volume of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to a person (such as medical or financial data), is treated as an aggravating factor when the Personal Data Protection Commission calculates the appropriate financial penalty.

48 See Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers" (WP 243) (13 December 2016) for examples of large scale processing and regular and systematic monitoring. See also Recitals 91 and 24 of the General Data Protection Regulation (Regulation (EU) 2016/679).

49 Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers" (WP 243) (13 December 2016) at pp 6–7.

50 Victoria Hordern, "The Final GDPR Text and What It Will Mean for Health Data" (Hogan Lovells, 20 January 2016). Data protection officers are also mandatory for public authorities but this is irrelevant for Singapore as public

(*continued on next page*)

professional DPOs based on their professional qualities and expert knowledge[51] (which their employer is obliged to help them maintain).[52] Second, although Art 37 of the GDPR does not establish the precise credentials of a DPO, Recital 97 suggests the level of expert knowledge "should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor".[53]

16 Presumably, under the PDPA, the above-mentioned sectors would benefit from engaging professional DPOs with a high level of expert qualities and knowledge based on a reasonable person's perspective. The exact qualities and knowledge of a professional DPO can then be determined by a combination of relevant data protection/privacy experience and certifications such as CIPM, CIPP or similar certificates, which correlate with the sensitivity, complexity and amount of data an organisation processes.[54] For example, a higher level of expertise will be required for hospitals that process large volumes of sensitive medical personal data. This requirement of right expertise is vital to Singapore's Smart Nation drive as the more Singapore organisations embrace and use technology that can process large amounts of personal data, the higher the expertise of their DPOs should be.

(2) Obligations

17 Under s 11(3) of the PDPA, DPOs are responsible for ensuring organisations comply with the Act. In this regard, DPOs need to advise the organisations, *inter alia*, how to put in place adequate protection for

---

authorities are excluded under the Personal Data Protection Act (Act 26 of 2012).

51 See Art 37 of the General Data Protection Regulation (Regulation (EU) 2016/679).

52 "Guide to the General Data Protection Regulation" (Bird & Bird, 2016) at p 33.

53 Rita Heimes, "Top 10 Operational Impacts of the GDPR: Part 2 – The Mandatory DPO" (International Association of Privacy Professionals, 7 January 2016).

54 Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers" (WP 243) (13 December 2016) at p 11.

personal data in their possession and/or control, develop and implement privacy policies and practices, and ensure consent has been obtained and proper notification given before the collection, use and disclosure of personal data. The obligations of DPOs should be based on a reasonable person standard. Although s 11(3) is not prescriptive of the precise requirements, one can take reference from Art 39 of the GDPR that a reasonable person would expect DPOs to advise their colleagues and monitor their organisation's privacy law/policy compliance via training and awareness raising, running audits, advising regarding DPIA and co-operating with supervisory authorities.[55] DPOs should also be involved from the earliest stage in all data protection issues especially for DPIA and PBDD. Where appropriate, the organisations should develop guidelines to set out when the DPO must be consulted.[56] As mentioned, if K Box had employed a DPO who conducted audits, DPIA and training, the data breach might not have occurred. The $50,000 financial penalty also took into account the unco-operativeness of K Box. Indeed, unco-operativeness and co-operativeness are listed as aggravating and mitigating factors in the *Advisory Guidelines*[57] *on Enforcement of the Data Protection Provisions*.[58] As such, if K Box had a DPO at the material time, it would have provided the necessary assistance to the PDPC during the investigation.

(3) Empowerment

19 It stands to reason that DPOs need to be sufficiently empowered in order for them to fulfil their obligations to a reasonable level as many of the obligations discussed above could not be discharged adequately without adequate empowerment. For example, it is fatuous to argue that a DPO can put in place a reasonable IT security system to protect personal data if the organisation does not provide sufficient funding or manpower, or that a DPO conducts himself and discharges his role impartially when he is under

55 "Guide to the General Data Protection Regulation" (Bird & Bird, 2016) at p 33.

56 Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers" (WP 243) (13 December 2016) at p 13.

57 Guidelines are not legally binding, but provide persuasive guidance in the interpretation, implementation and compliance of the Personal Data Protection Act (Act 26 of 2012). See s 49.

58 21 April 2016. See paras 25.2.3 and 25.3.5.

the direct supervision of or has to take instructions from the sales director in relation to data protection matters. Therefore, it cannot be gainsaid that an adequately empowered DPO ought also to be part of the senior management team, entrusted with the responsibility and provided with the resources that he needs in order to discharge his responsibilities.

20 Drawing lessons from the GDPR, Art 38 of the GDPR provides DPOs with the power to fulfil their obligations under Art 39: (a) adequate resources must be provided; (b) DPOs can operate independently of instruction and should report directly to the highest level of management (*eg*, the board of directors or the CEO or equivalent); and (c) DPOs cannot be dismissed or penalised for performing their task.[59] The first two are commonsensical as DPOs with only obligations and not the resources nor independence to fulfil them are only "paper tigers". Resources can refer to many things like manpower, continuous training or funds. Sometimes compliance and achieving targets of other departments might clash, and DPOs without direct access to the highest management could be circumvented or prevented from doing their job by other departmental heads holding high positions. Article 38 guarantees a certain degree of autonomy for DPOs to exercise their functions without interference.[60] That said, the immunity from dismissal might not be what a reasonable man would expect as Singapore has already put in place adequate employment laws and regulations to protect employees from unfair dismissal. For example, an individual who believes he has been subjected to unfair dismissal could lodge a complaint with the Tripartite Alliance for Fair and Progressive Employment Practices. Further, direct access to the highest management should be sufficient for DPOs to function without fear or favour. Another reason against having immunity from dismissal is it runs contrary to Singapore's capitalism and *laissez-faire* approach to its economy. Strong interference may cause more harm than good to the economy and that is not the intention of the PDPA.[61] Consequently, a reasonable person

59 "Guide to the General Data Protection Regulation" (Bird & Bird, 2016) at p 33 and Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers" (WP 243) (13 December 2016) at pp 13–16.

60 Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers" (WP 243) (13 December 2016) at pp 14–15.

61 Elaine Schwartz, "The World's Top and Bottom *Laissez-Faire* Countries" *Econlife* (2 May 2014).

would only deem points one and two to be necessary for DPOs to carry out their functions.

III. Conclusion

21 From the above analysis, organisations should appoint professional DPOs with precise obligations and qualifications to minimise the risk of data breach, and to co-operate with and demonstrate compliance to the PDPC. The requirements, obligations and power of DPOs can be determined from a reasonable person perspective. That said, the PDPC could consider elucidating these through guidelines so as to provide clarity for the industry. The clear responsibilities imposed on these professional DPOs will enable accountability to be ingrained in the Singapore data protection culture, and organisations' practices and policies. Concomitantly, compliance rates and trust between organisations and individuals would be improved. The professionalisation of the DPO industry would also contribute to Singapore's drive to be a Smart Nation, and global business and data hub.

REASONABLE SECURITY ARRANGEMENTS – RATIONALE, STUDY AND ANALYSIS*

Bryan TAN†
LLB (National University of Singapore); Advocate and Solicitor (Singapore), Solicitor (England & Wales)

Nathanael LIM‡
LLB (Singapore Management University); Advocate and Solicitor (Singapore)

I. Introduction

1 Section 24 of the Personal Data Protection Act 2012[1] ("PDPA") requires an organisation to "protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks"[2] ("Protection Obligation"). This article explores various decisions of the Personal Data Protection Commission of Singapore ("PDPC") pursuant to its administration and enforcement of the PDPA against various organisations, and identifies a number of factors the PDPC has considered in analysing whether an organisation has met the standards required of it under the Protection Obligation. By identifying these factors and case examples, it is intended that this will help to provide some practical guidance on complying with the Protection Obligation.[3]

2 A survey of these decisions reveals the recurrent theme that organisations are subjected to relatively high standards under the PDPA, which is in line with the general ethos of the PDPA – that ultimately,

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Partner, Pinsent Masons Mpillay LLP.

‡ Associate, Pinsent Masons Mpillay LLP.

1 Act 26 of 2012.

2 Personal Data Protection Act 2012 (Act 26 of 2012) s 24.

3 A non-exhaustive list of security measures an organisation should consider is included as an appendix to this article.

organisations are well placed to bear the responsibility of protecting personal data.

II. Personal Data Protection Commission Advisory Guidelines and section 24

3 As recognised in the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[4] released by the PDPC[5] ("Advisory Guidelines"), there is no one size fits all solution to determine what amounts to "reasonable security arrangements". What is reasonable and appropriate will depend on factors such as (a) the nature of the personal data; (b) the form in which the data are stored (*eg*, physical or electronic); and (c) the possible impact in the case of a breach. Organisations should therefore consider this in designing and organising their security arrangements.

4 A helpful starting point for any organisation will be the four "best practices" identified in the Advisory Guidelines – an organisation should ensure that it (a) has adequate training for its personnel; (b) has robust policies and procedures for data security; (c) has crisis management procedures for breaches; and (d) undertakes risk assessments occasionally. The Advisory Guidelines also contains helpful examples of administrative and physical measures an organisation may use to protect personal data. An example of the former is to require employees to be bound by confidentiality obligations in their employment agreements, and an example of the latter is to store confidential documents in locked file cabinet systems.

5 As a final point before moving on to the next section, it should also be noted that while data intermediaries may have a smaller set of obligations under the PDPA,[6] they are still obliged to comply with the Protection Obligation.

---

4 Revised on 15 July 2016.

5 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) ch 17.

6 Under the Personal Data Protection Act 2012 (Act 26 of 2012), a data intermediary is an organisation which processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is

(*continued on next page*)

III. Reasonable security arrangements

6 Organisations are expected to have security solutions and measures which provide comprehensive protection for an organisation's personal data in totality. Basic security solutions, such as the deployment of firewalls and anti-virus software, are common measures taken to secure personal data, but these measures alone may not always be found to be adequate to meet the requirements of the Protection Obligation.[7]

7 The following describe a number of practical examples, highlighted by the PDPC, which organisations should take note of in complying with the standards required of them under the Protection Obligation.

A. Implementing a data handling policy and transfer of data

8 Organisations are expected to have and enforce robust policies which set out proper practices to ensure that personal data are handled securely. Data handling policies should address multiple aspects of how personal data are handled, including how such data are stored, their transmission within and out of the organisation (for example, with third-party data processors), and identifying or appointing a data protection officer to oversee its implementation. A data handling policy is the starting point and a must-have for any organisation handling personal data. That being said, an organisation should be careful not to be lulled into a false sense of security even if it has a data handling policy, because unless such policy is effectively implemented and enforced, this would be insufficient to meet its obligations under the PDPA.

9 In relation to the transfer of data, organisations will do well to heed the observations of the PDPC:[8]

> [R]easonable or adequate security arrangements when transferring personal data must at least involve a process where the personal data is reasonably protected from unauthorised access or interference, until the personal data

---

evidenced or made in writing. For example, human resource administration and management service providers, to whom organisations may outsource payroll or employee data administration tasks, are likely to be considered data intermediaries.

7 See *The Institution of Engineers Singapore* [2016] SGPDPC 2 at [34].

8 See *My Digital Lock Pte Ltd* [2016] SGPDPC 20 at [25].

reaches its intended destination or recipient where other security arrangements on storage would apply.

One practice where organisations have commonly been found to fall short is the transmission of personal data without any password protection or encryption. The PDPC has expressly noted that the "practice of sending large volumes of … personal data via unencrypted email is a vulnerability" and this is one factor that would go towards a finding of whether or not the organisation has sufficiently protected the personal data.[9] The better practice would be to transfer personal data within the organisation's secured e-mail system, or at the very least ensure any documents containing personal data are password protected or encrypted.

10 To achieve this, organisations must ensure that they (a) have adopted the necessary technical capabilities to be able to provide such security measures; (b) understand such measures; and (c) properly considered what form of protection is necessary. At the basic level, organisations should protect attachments containing personal data (for example, an invoice) by use of a password. In doing so, organisations should bear in mind the other observations made in this article relating to the choice of passwords. Where necessary, for example where the risk of unintended disclosure is high or the personal data being handled are highly sensitive, organisations should further consider whether encryption measures are necessary. To elaborate briefly, as opposed to password protections, encryption (of either the attachment itself or the e-mail containing such personal data) scrambles the data into a non-readable format, such that even if an unintended recipient gains access to such data, the data cannot be read or processed unless properly decrypted first.

11 In any case, the observations of the PDPC clearly demonstrate that it is incumbent on organisations to consider the use of such measures in transmitting personal data. The use of open social media platforms, such as Facebook, to transfer personal data such as photographs, is also likely to constitute a breach of the Protection Obligation, since such personal data would be relatively easy to access given the open nature of open social media platforms.[10]

---

9 See *K Box Entertainment Group Pte Ltd and Finantech Holdings Pte Ltd* [2016] SGPDPC 1 at [29].

10 See *My Digital Lock Pte Ltd* [2016] SGPDPC 20 at [25].

B. Proper handling/use of administrative passwords and administrator accounts

12 Administrator accounts commonly allow access to personal data stored in an organisation's computer systems, and organisations are expected to exercise care in how administrator passwords and accounts are handled in order to prevent any unauthorised access to such personal data. Two errant practices identified by the PDPC in this regard include the failure to:

> (a) enforce the use of strong passwords (either as a matter of practice or by setting up a system which would automatically reject passwords which did not meet certain requirements);[11] and
>
> (b) exercise proper control and management of administrator accounts, for example, by not deleting unused accounts (which may have arisen from previous account holders such as employees who have left the organisation) or not having proper records of which employees are responsible for administrator accounts.[12]

13 From a more technical point of view, organisations should also avoid common security pitfalls associated with online password-account access. For example, passwords should not be simply stored as plain text as part of the PHP framework configuration file or SQL (as this would allow the password to be easily inferred with access to the right code or files), and should, at the very least, be encrypted. Even then, it would be wise for organisations to avoid weak-forms of encryption which are easily manipulated – the PDPC has expressed its reservations in one instance for example regarding the use of the MD5 message-digest algorithm, noting that it was a "commonly used cryptographic hash function" which "could be easily attacked with password tables by any motivated individual".[13]

---

11 See, *eg*, *Smiling Orchid (S) Pte Ltd* [2016] SGPDPC 19 at [49] and [50]. See also *K Box Entertainment Group Pte Ltd and Finantech Holdings Pte Ltd* [2016] SGPDPC 1 at [26] – although specific to this example, it would be helpful to note that it was briefly alluded to that a strong password would contain at least eight alphanumeric characters, with one capital and one special case character.

12 See *Smiling Orchid (S) Pte Ltd* [2016] SGPDPC 19 at [50].

13 See *Fei Fah Medical Manufacturing Pte Ltd* [2016] SGPDPC 3 at [19].

C. Conducting vulnerability tests and audits

14 It is incumbent on organisations to conduct vulnerability tests and audits on their systems in order to highlight any security vulnerabilities which may compromise the security of personal data. Organisations should also conduct intrusion/penetration testing to test how robust security measures put in place are. On more than one occasion where an organisation's systems have been compromised (for example, by a hacking attack), the PDPC has made express observations on the organisation's failure to conduct vulnerability audits or penetration tests which would have allowed them to rectify any vulnerabilities and prevented the unauthorised access. It is also probable that organisations are more likely to be found in breach of their Protection Obligation when a data breach arises from more common vulnerabilities, such as cross-site scripting[14] or SQL injection,[15] since such vulnerabilities could have been easily identified by vulnerability scans (and subsequently rectified).

15 Organisations will also need to take proper measures to address the root of any vulnerability in their system once identified. Superficial and stop-gap measures, for example, simply changing administrator passwords, making minimal changes to the underlying system code, or even moving to a new database may be found to be inadequate if they fail to address the root cause of any vulnerability.[16] To this end, organisations must dutifully invest in the proper corrective measures in the event that any system vulnerabilities are noted in order to comply with the Protection Obligation.

D. Securing accessible online data

16 It is not uncommon for organisations to store large amounts of personal data which are accessible online, and organisations must take reasonable security arrangements in relation to the access of such online data. Organisations usually provide their customers access to their personal data through an organisation's website or online account, and when personal data are retrievable through online access, organisations should be wary of some the common pitfalls observed by the PDPC:

---

14 See *The Institution of Engineers Singapore* [2016] SGPDPC 2 at [32].

15 See *Metro Pte Ltd* [2016] SGPDPC 7 at [15].

16 See *Smiling Orchid (S) Pte Ltd* [2016] SGPDPC 19 at [47].

(a) When unique identification numbers ("UIN") are used as a form of identification and access to a customer's online account, such numbers should not be easily manipulated such that an individual could easily derive UINs. For example, if UINs are simply issued sequentially, an individual could easily derive another individual's UIN by changing the final number(s) of his own (or a known) UIN. Likewise, where UINs are generated from a customer's date of birth or personal identity number, this may be considered a relatively weak form of security as UINs could be derived through number generation tools once other information is obtained.[17]

(b) Similar principles also apply to the uniqueness of the URL of web pages where personal data are stored. For example, it is not uncommon that a customer receives an online receipt of a purchase made online, which may contain personal data such as credit card details or mailing addresses. Organisations should be careful in ensuring that such web pages are not easily accessible by the clever manipulation of the URLs (similar to the above example, one clear instance of this is where the only difference between such web page URLs are the last few numbers of the URL such that by knowing one web page URL, an individual could easily derive the URL of other similar web pages), as this would likely be an inadequate form of protection and fall short of the requirements under the Protection Obligation.[18]

(c) Organisations should also be careful where online forms are used in the context of either accessing or collecting personal data. Where online forms have auto-fill capabilities enabled, this may run the risk of displaying previous personal data filled in by another customer. Organisations should also exercise extra caution to ensure that such forms do not provide access to data collected from other customers as well, for example, by inadvertently allowing access to the collective database through a link found on the form. Organisations must also keep in mind their other obligations under the PDPA, such as the obligation not to collect more data than what is required (which

17 See *ABR Holdings Ltd* [2016] SGPDPC 16.

18 See *Fu Kwee Kitchen Catering Services and Pixart Pte Ltd* [2016] SGPDPC 14 at [16].

would be relevant in the design of such forms), and the obligation only to retain data for as long as reasonable.

17 While the above examples are relevant to personal data stored virtually, the principles apply equally to physical access to personal data. When personal data are recorded in physical record books for example, organisations have a duty to ensure that these physical record books are stored properly and that access to them is controlled in order to prevent the unauthorised disclosure of personal data.[19]

E. Proper security awareness and delegation of responsibilities to third parties

18 Organisations very often work with third-party service providers in dealing with personal data, and organisations are expected to properly manage any delegation of responsibilities for the protection of personal data to such third-party service providers. The Advisory Guidelines state that:[20]

> [I]t is important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in their written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question including whether one organisation is to process personal data on behalf of and for the purpose of the other organisation.

19 In relation to the handling of personal data, third-party services often feature in *back-end support* processes, such as the design of an organisation's information technology ("IT") system, or *front-end operational* processes, such as sending out mailers or marketing material to an organisation's customers. In either case, organisations should ensure that their written contracts with such third parties (or a relevant document such as the scope of works/services) detail how the third-party service provider is responsible for the protection of personal data.

20 It is no excuse for organisations to claim ignorance over the security solutions in their computer systems where this has been outsourced to a

---

19 See *Spear Security Force Pte Ltd* [2016] SGPDPC 12.

20 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) ch 3, at para 6.21.

third party. On the contrary, such ignorance is more likely to be construed as a "lack of awareness" towards data protection, and is likely to fall short of the standards required under the Protection Obligation. Where a third party is engaged to support an organisation's IT functions such as the designing of an organisation's system/website or the hosting of an organisation's data on an online server, an organisation must clearly contemplate how data protection is to feature as part of such services, and if the intention is so, the organisation should clearly indicate that the security of such systems fall under the scope of work of the third party; an organisation cannot simply assume that the third party is responsible for this, and must manage its third parties such that proper security for personal data is provided.[21] These principles apply equally to third-party service providers who further outsource or subcontract any development work to another third party – it would be insufficient for such third-party service providers to simply claim that they had outsourced their work; they must still ensure that the final product contains sufficient security measures for data protection.[22]

21 Likewise, where a third party handles personal data for an organisation, the organisation must ensure that such third-party vendors have proper security measures in place, and the PDPC has gone as far as to state that an organisation must exercise sufficient supervision over a third party's workflow in the processing of an organisation's personal data. In finding that an organisation had breached the Protection Obligation, the PDPC observed that it was insufficient to leave a third party to implement its own measures, and the organisation should have "considered what requirements it would want to implement to ensure that the personal data was appropriately protected".[23]

22 A positive example will be helpful to illustrate how an organisation may discharge its duties to properly manage its third parties. In one case,[24] the PDPC observed that an organisation had:

---

21 See *K Box Entertainment Group Pte Ltd and Finantech Holdings Pte Ltd* [2016] SGPDPC 1 at [29].

22 See *Smiling Orchid (S) Pte Ltd* [2016] SGPDPC 19 at [23].

23 See *Challenger Technologies Ltd and Xirlynx Innovations* [2016] SGPDPC 6 at [34].

24 See *Aviva Ltd and Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC 15.

(a) entered into an agreement with the third-party service provider to put in place adequate security policies, procedures and controls to protect the confidentiality and security of its customers;

(b) provided a standard operating procedure as to how its third-party service provider was to handle its personal data, and required the third-party service provider to seek final confirmation from the organisation before the personal data were disclosed;

(c) carried out annual inspections and review of the third-party service provider to ensure that it was adhering to its security procedures; and

(d) conducted annual on-site inspections to verify the third-party service provider's IT security and business protection measures.

23 As a result of the organisation's efforts, although a data breach had occurred, the PDPC found that the breach was on the part of the third-party service provider, and not the organisation.

F. Processes to deal with human error (including proper staff training)

24 The PDPC has also noted that where personal data are handled by individuals, organisations should put in place processes which will help to deal with human error as part of its security measures. For example, where recipients are to receive individual personal data pursuant to a recipient address list, simple measures such as sample proof-reading (where the sample size is appropriate to the total number of recipients) would be a reasonable security arrangement to have in place to help avert potential mistakes.[25] Removing sensitive information from previous threads and removing attachments which may not be relevant to the immediate e-mail (in order to prevent accidental disclosure to unintended recipients) are also good practices an organisation can adopt to mitigate human error.[26]

25 As already stated in the Advisory Guidelines, sufficient training should also be provided for employees so that they are aware of such good practices and the proper security measures to which they will need to adhere in protecting personal data.

---

25 See *Challenger Technologies Ltd and Xirlynx Innovations* [2016] SGPDPC 6 at [30].

26 See *Singapore Computer Society* [2016] SGPDPC 9 at [8].

G. Handling breaches by proper notification and rectification methods

26 An organisation's crisis management procedures upon a breach also form part of its reasonable security arrangements. If a breach occurs, organisations should take efforts to notify affected individuals, as well as take proactive corrective measures to improve their data protection measures (such as engaging a new IT vendor or hiring the services of a data protection consultant), as soon as possible. These steps have been noted by the PDPC in various instances, and are likely to be considered as mitigating factors when deciding the severity of any penalties which may be imposed.[27] Organisations should also aspire to respond as quickly and co-operate as far as possible to and with any investigations by the PDPC in relation to any breach, lest any delay be taken as an organisation's insouciance towards its Protection Obligation under the PDPA, which may lead to more severe penalties for any breach.[28]

IV. Conclusion

27 The enforcement actions of the PDPC are a clear indication to organisations that they are to take their obligations under the PDPA nothing short of seriously. Given the multiple illustrations of where an organisation could potentially fall short of taking "reasonable security arrangements", it is clear that the primary responsibility of the protection of personal data falls squarely on the shoulders of such organisations. As observed by the PDPC, "the occurrence of a data breach is a *prima facie* indication that [an organisation] had not fulfilled its responsibilities in respect of processing and sending personal data".[29] There are plenty of lessons to learn from the case examples as discussed above, and organisations will do well to review their internal processes and invest meaningfully in data protection in order to ensure that they comply with their obligations under the PDPA.

---

27 See *Challenger Technologies Ltd and Xirlynx Innovations* [2016] SGPDPC 6 at [38].

28 See *Fei Fah Medical Manufacturing Pte Ltd* [2016] SGPDPC 3 at [33].

29 See *Challenger Technologies Ltd and Xirlynx Innovations* [2016] SGPDPC 6 at [28].

APPENDIX

CHECKLIST

The following is a non-exhaustive "checklist" of reasonable security arrangements covered by the cases discussed above which organisations should consider implementing or improving upon, in evaluating their own practices:

Action	Fulfilled?
Secure transmission of data – Transmission of personal data is via secured channels such as an organisation's secured e-mail server, and not over personal e-mail accounts.	
Proper control and management of administrator accounts – A record of which employees are given administrator rights is kept, and only given to employees who require such rights. Redundant administrator accounts are deleted.	
Password management – The use of strong passwords is enforced. Strong passwords would generally contain more than eight, both alpha and numeric, upper and lower case, and special characters.	
Secure password-account access – Passwords which allow online account access are stored properly, encrypted and not easily accessible through digital files.	
Vulnerability tests – Vulnerability and penetration audits/tests are conducted occasionally to test security measures.	
UINs and URLs – UINs and URLs which allow access to personal data are randomised as far as possible so as to prevent them from being easily inferred from each other.	
Physical storage – Physical documents which contain personal data are stored properly to prevent unauthorised access to such documents.	
Contracts with third parties – The relevant contracts clearly express security obligations and responsibilities if these are to be handled by a third-party service provider.	
Third-party security operating procedure – A clear operating procedure to ensure security is documented for third parties, to whom personal data security has been	

outsourced, to follow. Audits or inspections are carried out occasionally to ensure that such third parties abide by these procedures.	
Processes to deal with human error – Procedures such as sample-checking or proof-reading practices are put in place to deal with human error.	
Proper training – Employees undergo training to familiarise themselves with data handling policies and good data handling practices.	
Notification – A system is put in place such that individuals whose personal data have been compromised are alerted immediately.	

A PRACTICAL APPROACH TO DATA INTERMEDIARIES*

Alexander YAP Wei-Ming†
MA (Keble College); Advocate and Solicitor (Singapore), Solicitor (England & Wales)

Cheryl LIM Qian Yi‡
LLB (King's College London); Advocate and Solicitor (Singapore)

Claudice WEE Li Yun§
LLB (King's College London); Advocate and Solicitor (Singapore)

I. Introduction

1 With the advent and widespread penetration of mobile computing and the potential surrounding the "Internet of Things", the need for adequate protection for data (particularly personal data) has never been more crucial. Recent years have witnessed a constant stream of new "smart" technologies, and an upsurge of enterprises making the switch from traditional brick-and-mortar storefronts to developing some kind of online presence.[1] Inevitably, individuals are exposed to an ever-increasing number of avenues and means by which their personal data in various forms[2] are being collected, used, processed and disclosed. This has in turn resulted in a growing concern regarding how organisations use and protect the personal

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Partner, Allen & Gledhill LLP.

‡ Senior Associate, Allen & Gledhill LLP.

§ Associate, Allen & Gledhill LLP.

1 In a recent survey on infocommunications usage by enterprises conducted in 2015 by the Infocomm Development Authority of Singapore, the proportion of enterprises using mobile services (including SMS/MMS, mobile websites and mobile applications) to engage consumers saw a significant uptick from 43% in 2013 to 61% in 2015.

2 In addition to what is conventionally considered personal data, mobile applications may now collect a vast range of data from biometric data, financial data and location data.

data under their control, which has no doubt been exacerbated by the various large-scale and high-profile data breaches.[3]

2 The introduction of the Personal Data Protection Act 2012[4] ("PDPA") in Singapore was a great step forward in building trust and assuaging fears relating to the protection of personal data. However, the practical application of the PDPA arguably raises the question of the appropriate apportionment of liability between organisations and their data intermediaries for compliance with the PDPA.

3 A key example of this is the operation of s 4(2) read with s 24 of the PDPA, which provide that "data intermediaries" (typically service providers), who process personal data on behalf of and for the purposes of another organisation (such organisations hereinafter referred to as "data controllers") pursuant to a contract evidenced or made in writing, nevertheless owe an obligation to protect the personal data being processed. The operation of this "secondary liability" works to keep data processers accountable even when not collecting, using or disclosing personal data for their own purposes. This was the case in the recent enforcement against Global Interactive Works, who, on behalf of Cellar Door, simply designed and developed Cellar Door's business website and provided backups of the website and Cellar Door's customer database.[5] The effectiveness of this provision in ensuring that personal data are protected at the various levels is evident, especially considering that organisations now only occasionally work on their own and instead often work in tandem with other systems or software providers; especially given the ubiquity of, and the comparatively reduced cost of, cloud computing. Nevertheless, s 4(2) implicitly recognises that such "secondary liability" is different in nature and less extensive than the corresponding "primary liability" of the data controller, and for this reason does not seek to impose data protection obligations on the data

3 Most recently, Yahoo reported in September 2016 and December 2016 two separate data breach incidents occurring in late 2014 and August 2013 respectively, which affected over one billion user accounts in total. Vindu Goel & Nicole Perlroth, "Yahoo Says 1 Billion User Accounts Were Hacked" *The New York Times* (14 December 2016).

4 Act 26 of 2012.

5 *Cellar Door Pte Ltd and Global Interactive Works Pte Ltd* [2016] SGPDPC 22.

intermediary other than those in respect of the protection and retention of personal data.[6]

4 Whilst the effort to balance the accountability of data intermediaries against the amount of control they realistically exercise is commendable, it is often not clear when a service or software provider is to be considered a "data intermediary" in the first place. For example, while it may be a fair argument to impose liability on a service provider such as Global Interactive Works who as part of its engagement stored the customer data of Cellar Door on its servers (which activities fall squarely within the definition of "processing'" under the PDPA), the same argument is more challenging in the context of a software provider who provides a more "hands-off" service and has little or no contact with an organisation, save that the organisation made an off-the-shelf purchase of software developed by the provider.

5 This article seeks to engage in a discussion on the types of activities that may cause organisations to become data intermediaries, using as a backdrop the typical developmental "life cycle" of systems.

II. Data intermediaries

6 The extent to which a service provider can be held liable for lapses in compliance with the requirements of the PDPA will often depend on whether that service provider may be regarded as processing data on behalf of another organisation as a "*data intermediary*" under the PDPA. Clearly, where an organisation processes data not as a data intermediary but on its own behalf and for its own purposes, s 4(2) of the PDPA will not apply and the organisation will be subject to the full suite of data protection obligations under the PDPA. Conversely, where the service provider does not process personal data at all, it will not be subject to any of the data protection obligations under the PDPA.

7 On a plain reading of the PDPA, the question of whether or not an organisation is a data intermediary turns on whether it "*processes*" personal

6 For instance, a data intermediary need not be concerned with the data protection obligations under the Personal Data Protection Act 2012 (Act 26 of 2012) relating to the obtaining of consent, which are solely the responsibility of the data controller.

data on behalf of and for the purposes of another organisation. This is a question of fact which requires consideration of the following issues:

(a) Activity-oriented characterisation exercise – The term "processing" is afforded a wide scope under the PDPA as including any act of recording, holding, organisation, adaptation or alteration, retrieval, combination, transmission, erasure or destruction. However, practically speaking, whether a service or software provider is regarded as a processor of personal data will largely turn on the degree of control that the provider has over the system and/or software it provides or operates, as well as the degree of control it has over the "systemic processing of personal data, with its attendant collection, use and disclosure".[7]

(b) Purposes of processing – As a "data intermediary" collects, uses, processes and/or discloses personal data on behalf a data controller who has engaged its services, it stands to reason that the "data intermediary" must only carry out all collection, use, processing and/or disclosure for the purposes of the organisation.

III. Life cycle of systems development

8 From a practical standpoint, in this article, the issue will be examined in the context of the various stages of systems development. For the purposes of this article, the life cycle of a system or software may largely be grouped into the following stages:

(a) the design and development stage, which involves:

(i) plans being laid out *vis-à-vis* the specifications of the system, which concern, *inter alia*, the physical construction, hardware, operating systems, programming, communications and security issues of the system;[8] and

(ii) the execution of the plans and specifications, where software and/or system developers generate and refine the

7 Daniel Seng, "Data Intermediaries and Data Breaches" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Singapore: Academy Publishing, 2014).

8 Margaret Rouse, "Systems Development Life Cycle" <http://searchsoftwarequality.techtarget.com/definition/systems-development-life-cycle> (accessed 15 May 2017).

software codes to build the system, and design the user experience and interface aspects of the system;[9]

(b) the testing, implementation and deployment stage, where the finished product is tested for functionality, performance and integration with other products and/or previous versions of the system with which the new system needs to communicate, before the system is finally formally rolled out to end-users in the market;[10] and

(c) the operation and maintenance stage, where the product, having been launched, is administered and maintained.

9 This article will consider each of the above stages in the context of services that an organisation will typically utilise at the particular stage of development.

A. Design and development stage

10 The central question in the context of the design and development stage would be whether or not software or web developers should be held liable solely for data breaches involving personal data occasioned by the poor design of the software, website or application in question. As mentioned above, in the authors' view, this would largely turn on the degree of control that the developer has over the system or software it provides, as well as the degree of control over the "systemic processing of personal data".

11 An interesting recent example is that of *JP Pepperdine Group Pte Ltd*[11] ("*JP Pepperdine*"), where Ascentis, a web designer, was held not to be the data intermediary of JP Pepperdine as its role was limited to designing the relevant web page for JP Pepperdine according to the instructions of the latter. In particular, the web page was designed without any security measures as *per* JP Pepperdine's specifications, and was originally intended purely for internal purposes and temporary use. In making this finding, it is

9 Kaye Morris, "Steps in the System Development Life Cycle" <http://smallbusiness.chron.com/steps-system-development-life-cycle-43241.html> (accessed 15 May 2017).

10 Kaye Morris, "Steps in the System Development Life Cycle" <http://smallbusiness.chron.com/steps-system-development-life-cycle-43241.html> (accessed 15 May 2017).

11 [2017] SGPDPC 2.

not entirely clear if the Personal Data Protection Commission ("PDPC") intended to draw a line in the sand with respect to pure development work (*ie*, that developers would not be considered data intermediaries *solely* on the basis that the web page or application they developed processes personal data), or whether the PDPC was making a more nuanced finding taking into account the lack of control and agency on the part of Ascentis in the development process. The former interpretation is more likely given the fairly narrow definition of data intermediary (as one which "processes" personal data on behalf of another) and given the PDPC's finding that "there was no evidence" that Ascentis processed any personal data on behalf of JP Pepperdine.

12 As such, it is unclear how the term would apply in the context of a traditional software licensing model, where the software developer provides the customer with software which the customer installs and runs on its own infrastructure, particularly where the software in question is "client-neutral" or "purpose-agnostic". In the light of *JP Pepperdine* (discussed above), such developers would likely not be regarded as data intermediaries by the PDPC. Nevertheless, given the legislative intent behind s 4(2), it is noted that there might be circumstances (*eg*, where the processing of personal data is central to the software or application, or where the developer knows or reasonably ought to know that there is a high likelihood that the software or application will be used for the collection, use or disclosure of personal data) where there are good reasons to impose basic obligations/standards on the developer *vis-à-vis* the security of the software or application in question. In this regard, it might be worth considering whether the definition of "data intermediary" should be widened (for instance, to encapsulate not only those who undertake the actual "processing" of data but those who provide software or facilities for the processing of personal data) and the "Protection" Obligation under s 24 correspondingly revised.

13 Arguably, where what is being provided is "Software as a Service" ("SaaS"), there is greater scope for the provider to be considered a data intermediary. Since the provider typically hosts applications and data (which may include customer data and personal data) and makes them available to the customer over the Internet, the security measures to be implemented by the provider should be at least as rigorous as those applied by the customer. Perhaps one of the greatest concerns about cloud computing are privacy and security, as the data controller hands control and possession over important data to the provider. And indeed, it is in the

interest of SaaS providers to have reliable security procedures in place as data breaches could be fatal to the reputations of such providers. It is argued that in SaaS situations, where there is a high likelihood that the software or application in question will be used to process personal data (*eg*, in the case of web-based e-mail providers such as Gmail or Yahoo! Mail), the provider should be held accountable as a data intermediary for any data breaches which arise from poor or inadequate security measures.

14 An interesting question arises in respect of social media websites such as Facebook or Twitter, which host content on behalf of individuals and enable them to communicate and broadcast content. Such providers are *prima facie* data intermediaries to users who are businesses as they have "outsourced" the collection and retention of their data (including personal data) to such sites.[12] To the extent that any such personal data are shared or disclosed at the direction of the user (for instance, users may choose their own privacy settings and choose who can see specific parts of their profiles and the information they have shared, or who can locate them through searches), the site deals with the data as a data intermediary. Nevertheless, to the extent users share personal data not just between themselves but also with the site, and the site utilises the data for extraneous purposes (*eg*, for the purposes of the site conducting data analytics, or for targeted advertising), the question of who controls dealings with the personal data is less clear-cut. It is possible that providers of such sites might concurrently be acting both as data intermediaries and as data collectors with respect to the same data set, depending on the purposes for which personal data are being processed in a particular instance.

15 Whilst not strictly on point, it is worth emphasising that whether or not they are considered "data intermediaries", software and web developers and designers play a key role not only in the security aspects but in working with the website or application provider to meet data protection and privacy requirements. Organisations should be made aware that the design and development stage is the ideal stage to start assessing data protection and privacy matters so that they are factored into the design and implementation of the relevant website or application.

---

12 Daniel Seng, "Data Intermediaries and Data Breaches" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Singapore: Academy Publishing, 2014).

B. Integration, testing and implementation stage

16 Implementation often involves other parties such as platform providers (*eg*, providers of operating systems, hardware or devices and/or other software platforms), providers of other applications or facilities with which the application will interface and associated app-stores which publish or sell the application.

17 Where a data breach is due to security issues with the provider's platform (*eg*, the operating system), questions arise as to whether such a provider should be considered a data intermediary and subject to the obligation to protect personal data by making reasonable security arrangements notwithstanding the fact that the provider is not "processing" the data in the conventional sense. It is worth noting that typically such providers have standard terms and policies which the software or application provider signs up to, and the platform provider has little or no control over the actual software or application and the type of processing of personal data which is involved.

18 Having regard to *JP Pepperdine*, it is unlikely that such platform or hardware providers will be regarded as data intermediaries by the PDPC (see the analysis above).

C. Operation and maintenance stage

19 After the software, website or application is launched, it is common for various third parties to be involved in managing or maintaining the software, website or application, or for storing, administering or analysing data collected.

20 Such parties may be considered data intermediaries where their operations involve the "processing" of personal data. It is worth noting that not all third parties appointed to assist in the management or maintenance of the software, website or application or the data will need access to personal data (if the third party's role is data analysis or maintenance, the software or application provider should consider whether information can be anonymised or whether test data can be provided).

21 For instance, in *Propnex Realty Pte Ltd*,[13] although P&N Holdings and the organisation being investigated shared a common information technology ("IT") infrastructure, with P&N Holdings maintaining and operating the common IT infrastructure and providing IT support to the organisation, there was no evidence to suggest that P&N Holdings processed any personal data on behalf of the organisation. On the other hand, in *Singapore Telecommunications Ltd and Tech Mahindra*,[14] where the maintenance and support services being provided by Tech Mahindra to Singtel involved the maintenance and updating of customer profiles in the relevant database, Tech Mahindra was found clearly to be acting as a data intermediary of Singtel.

IV. Extraterritoriality of the Personal Data Protection Act

22 At this juncture, it is worth saying a few words about the territorial reach of the PDPA, which would be relevant to service providers providing services from different jurisdictions. Whilst the PDPA is very new and there are no reported judgments on the issue, there are some reasons why the PDPA may be regarded as having limited extraterritorial effect from a conservative perspective.

23 Whilst the PDPA is not expressly stated to have extraterritorial effect, the provisions of the PDPA clearly envisage its applicability to organisations outside of Singapore. For example, Pts III and VI of the PDPA are directed towards "organisations", which are defined in s 2(1) to include companies: "*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*" [emphasis added], and s 52, which deals with offences by bodies corporate, also envisages the promulgation of regulations "to provide for the application of any provision of this section … to any body corporate … *formed or recognised under the law of a territory outside Singapore*" [emphasis added]. Furthermore, the provisions which impose obligations on "organisations" do not exclude organisations outside of Singapore or limit "individuals" (whose personal data are protected) to Singapore residents or any other class

13 *Propnex Realty Pte Ltd* [2017] SGPDPC 1.

14 *Singapore Telecommunications Ltd and Tech Mahindra (Singapore) Pte Ltd* [2017] SGPDPC 4.

of individual. Indeed, "individuals" are defined in s 2(1) to include "any natural person, whether living or deceased".

24 Nevertheless, these provisions are better explained by the PDPA needing to reach outside of Singapore to capture Singapore companies or entities which may seek to circumvent the PDPA. It is also noted that if the PDPA has extraterritorial effect, every organisation in the world would strictly speaking need to, *inter alia*, appoint a "data protection officer" and implement data protection policies compliant with the PDPA which is unlikely to have been the intention of the Singapore Parliament. As regards service providers registered and located outside Singapore, enforcement would also inevitably be an issue.

V. CONCLUSION

In a world where increasingly more complex and interconnected networks gather, share and transmit detailed information, the need to ensure adequate protection for personal data at all levels is pressing. Whilst the regime under the PDPA aims to calibrate the obligations owed by organisations in respect of personal data to the amount of control exercised by that organisation over the personal data, it is often not apparent whether a particular organisation is acting as a data intermediary. In particular, where the collection, use and disclosure of personal data is conducted through web pages or applications, the question of who is a data intermediary becomes even less clear. Whilst it would appear that the PDPC does not consider pure development work as "processing" within the meaning of the PDPA, it can be argued that there might be instances where it would be appropriate to hold a developer liable for data breaches solely arising from poor design of the website or application in question. Given how integral the work of software and web developers and designers are where security is concerned, it might be worth revisiting the definition of "data intermediary" and what it means to be a "data intermediary" – the key question being: who has the responsibility under the PDPA to ensure that websites/applications have applied "reasonable security arrangements".

THE ACCESS OBLIGATION AND ITS PURPOSE*

LEE Soo Chye†
LLB (National University of Singapore);
Advocate and Solicitor (Singapore)

"A good reputation is worth more than money."[1]

I. Introduction

1 The Personal Data Protection Act 2012[2] ("PDPA") was enacted on 15 October 2012. It comprises two main sets of provisions: Pts III–VIII which cover data protection ("Data Protection Provisions") and Pt IX which covers the "Do Not Call Registry" ("Do Not Call Provisions").

2 During the second reading of the Personal Data Protection Bill ("Bill"), then Minister for Information, Communications and the Arts, Associate Professor Dr Yaacob Ibrahim, highlighted that:[3]

> [P]ersonal data protection law will safeguard the individual's personal data against misuse by regulating the *proper management of personal data* … In formulating the Bill, we have sought to *balance* individual's interest with the need to keep compliance costs manageable for organisations. [emphasis added]

With reference to the Data Protection Provisions, Dr Ibrahim stated that "these rules are based on the principles of obtaining consent, specifying purpose and reasonableness".[4] In the concluding remarks to the

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors remain the author's own.

† Senior Partner, Aequitas Law LLP. Soo Chye would like to acknowledge the contribution of Wong Ee Vin towards the publication of the article.

1 Publilius Syrus.

2 Act 26 of 2012.

3 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

4 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

parliamentary debate, he said that "the [Bill] has taken the approach of protecting individual's personal data without imposing overly onerous requirements on organisations".

3 These broad principles are captured in s 3 of the PDPA, which states:

> The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises *both the right of individuals to protect their personal data* and *the need of organisations* to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. [emphasis added]

4 This paper is divided into five sections. Part II[5] will discuss the scope of the obligation imposed on organisations under s 21 of the PDPA ("Access Obligation").[6] Part III[7] will cover two exceptions – namely, paras 1(*j*)(ii) ("Disproportionate or Unreasonable Exception") and 1(*j*)(v) ("Frivolous or Vexatious Exception") of the Fifth Schedule to the PDPA – under which organisations will not be required to comply with the Access Obligation. Part IV[8] will explain how organisations should comply with the PDPA before concluding in Part V.[9]

II. Scope of Access Obligation

5 Section 21 (on the Access Obligation) and s 22 (the obligation to correct inaccurate personal data, or the "Correction Obligation") appear together under Pt V of the PDPA. Section 21(1) reads:

> Subject to subsections (2), (3) and (4), *on request of an individual*, an organisation shall, as soon as reasonably possible, provide the individual with:
>
> (*a*) personal data about the individual that is in the possession or under the control of the organisation; *and*

5 See paras 5–11 below.

6 Although this has generally been described as an obligation on the organisation to grant "access" to the individual requester, it may be better understood as an obligation to disclose the individual's personal data and certain information relating thereto to that individual or his authorised representatives.

7 See paras 12–31 below.

8 See paras 32–33 below.

9 See paras 34–35 below.

(*b*) information about the *ways* in which the personal data referred to in paragraph (a) *has been or may have been used or disclosed* by the organisation within a year before the date of the request.

[emphasis added]

6 With the legislative purpose for the PDPA so expressed during the parliamentary debates, it appears that s 21(1) is intended to allow an individual to know what personal data is in the possession or control of the organisation and how it has been used or disclosed. In addition, it enables individuals to correct the personal data (where necessary), and to verify that the organisation has used or disclosed the personal data only for the purposes for which it was collected, or as may be permitted under the Third and Fourth Schedules to the PDPA. Section 21(1)(*b*) and the grouping of the Access Obligation together with the Correction Obligation in the same part of the PDPA will appear to support this conclusion.

7 There are two instances in which an organisation may lawfully be in possession or control of an individual's personal data: either the individual has provided the personal data to it, or the organisation has obtained it from other sources. With s 21(1) of the PDPA, an individual can find out if the personal data the organisation possesses or controls is more than what he had consented for the organisation to collect, use or disclose, and if it is, what other personal data the organisation has of him that might have been collected, used or disclosed without his consent. In either case, it would be in the interest of the individual to ensure that the personal data in the possession or control of the organisation is correct, hence the right of the individual to request that personal data be corrected.

8 It is submitted that this is the extent of the individual's rights or interest that s 21(1) of the PDPA seeks to protect, bearing in mind the legislative intent to balance the needs of the organisation as well.

9 Ideally therefore, the request by the individual should state his purpose for that request. However, such a requirement is not explicitly stated in s 21.[10] Even if the individual makes a request without stating his

10 The Personal Data Protection Commission, charged with the authority to administer the Personal Data Protection Act 2012 (Act 26 of 2012) has, in its *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at para 15.11, suggested that a requester should

(*continued on next page*)

purpose, the organisation *must* provide to the individual his personal data and information as requested unless prohibited by the PDPA[11] or he is not required to do so under the Fifth Schedule.[12]

10 In reality, where there is a genuine desire of the individual to protect his personal data (either to ensure that his personal data is accurate or that the organisation has not collected, used or disclosed personal data other than that for which he has given his consent, or which the organisation is permitted to collect, use or disclose under the PDPA), any organisation would be hard-pressed to reject such a request.

11 The problem arises where the individual's request is not for the purposes mentioned above.[13] Are there grounds for the organisation not to accede to the request in such instances?

III. Exceptions under Fifth Schedule[14]

12 The two possible exceptions that may be applicable in such circumstances are: the Disproportionate or Unreasonable Exception and the Frivolous or Vexatious Exception in the PDPA.

13 Under the Disproportionate or Unreasonable Exception, organisations are not required to respond to a request "where the burden or expense of providing access would be *unreasonable to the organisation* or *disproportionate to the individual's interest*" [emphasis added].

---

provide details to assist the organisation in its search for the personal data requested. However, such guidelines do not have the force of law.

11 Personal Data Protection Act 2012 (Act 26 of 2012) ss 21(3) and 21(4).

12 Personal Data Protection Act 2012 (Act 26 of 2012) s 21(2).

13 See para 8 above.

14 In line with the legislative approach to balance the individuals' need for protection of their personal data and the needs of the organisations, there are various exceptions to the requirement in s 21(1) of the Personal Data Protection Act 2012 (Act 26 of 2012). It has been commented that these exemptions are so numerous that the right to access is considered "a very diluted right": *Data Protection Law in Singapore – Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2014) at para 5.60.

14 Under the Frivolous or Vexatious Exception, organisations are not required to respond to a request that is otherwise "*frivolous or vexatious*" [emphasis added].

A. The Disproportionate or Unreasonable Exception

(1) Personal Data Protection Act

15 It is pertinent to note that under the Fifth Schedule to the PDPA, the Disproportionate or Unreasonable Exception has two limbs (*ie*, unreasonable to the organisation or disproportionate to the individual's interests). As an illustration, an individual has provided the same personal data to two organisations, A and B. Organisation A is a huge multinational enterprise. Organisation B is a small enterprise. To meet the request of the individual under s 21(1), both organisations will incur a sum of say $10,000. The burden of this expense will *prima facie* be heavier on organisation B compared to organisation A given their relative sizes, and therefore may well be "unreasonable" to B but not to A. By extension of the illustration, just because the burden and costs of $10,000 is not unreasonable given the size of organisation A, it does not follow that that expense is proportionate to the individual's interests.

16 The question then arises as to whether the organisation can rely on this exception where the costs are "unreasonable" but not "disproportionate" to the individual's interests. Unfortunately, the use of the word "or" does create ambiguity as to whether it should be construed conjunctively or disjunctively.

17 There is no guidance in the PDPA on what is "unreasonable" or "disproportionate" or how the individual's interests in such a context should be measured. Nevertheless, it is submitted that a conjunctive interpretation of the word "or" would be more consistent with the legislative intent for the PDPA, which seeks to balance the needs of the individual and that of the organisation. The Disproportionate or Unreasonable Exception therefore calls for the organisation's burden or expense in the provision of access to be weighed against an individual's interest. It is submitted that the application of this exception must necessarily depend on the particular circumstances surrounding the request. These circumstances should include:

(a) Circumstances under which the organisation had collected the personal data. If the data is not properly collected according to ss 13 and 14 of the PDPA, then the organisation may not be able to argue that the burden or expense in the provision of the access is unreasonable. The organisation should not profit from its own wrongdoing; the prohibitive cost or burden of giving access should not be a sufficient justification to refuse access. Contrast this to where the requestor has provided that information or consented to the collection of that information: in such a situation, it is arguable that the organisation should not be required to incur any substantial expense to meet the request.

(b) Difficulty faced by the organisation in providing the information. However, if the organisation chooses to store the personal data collected in forms that are difficult and expensive to access/retrieve or has not taken steps to enable such personal data to be readily accessible without incurring substantial costs, then the fact that the organisation must incur exorbitant costs to meet the request cannot be a valid reason for not giving access.[15]

(c) The size of the organisation.[16]

(d) The cost of providing the information.[17]

---

15 See, *eg*, Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at para 15.21.

16 See *Elliott v Lloyds TSB Bank plc* [2012] EW Misc 7 (CC) (24 April 2012) at [15].

17 As part of the attempt to balance the needs of the organisation and the interests of the individual, the regulations do provide that the organisation can charge a reasonable fee for providing the personal data and information requested, including any incremental costs associated with responding to individual access requests as long as the fee reflects the time and effort required to respond to such a request. The Personal Data Protection Commission is also empowered to review the fees charged by an organisation in relation to requests under s 21 of the Personal Data Protection Act 2012 (Act 26 of 2012). In this regard, the Personal Data Protection Commission has provided guidance that the organisation should not charge for "costs that are necessarily incurred for the organisation to comply with the PDPA regardless of whether an access request was actually made": Personal Data Protection Commission, *Closing Note For Public Consultation Issued By the Personal Data Protection Commission on: Proposed Regulations Under the Personal Data Protection Act in*

(*continued on next page*)

(e) The conduct of the requester.[18] If the requester refuses to co-operate with the organisation by, for example, failing to answer reasonable clarifications sought by the organisation or unreasonably insisting on actions that may not be necessary to meet the purpose of the requester, the unreasonableness of the conduct of the requester should be a factor that is weighed against acceding to the request.

(f) The purpose for the request. If the purpose is expressed to be for correction and/or verification of the accuracy of the personal data, then as stated above, the organisation may be hard-pressed not to accede to the request. It is noted that the Disproportionate or Unreasonable Exception does not apply to the Correction Obligation.

(2) Practice in other jurisdictions

18 To date, there are no case authorities from the Singapore courts on the interpretation and application of the various provisions of the PDPA. While there are rulings on the Access Obligation by the PDPC (and some of these cases involved allegations that the requester was "creating [a] nuisance"[19]), unfortunately, by the time the matters went before the PDPC, the information requested for was no longer available. The issue of whether the Disproportionate or Unreasonable Exception or the Frivolous or Vexatious Exception were applicable in those instances was therefore not relevant for consideration by the PDPC.

19 In the UK, the Data Protection Act 1998[20] ("DPA") provides for a "disproportionate effort" exception[21] in relation to giving individuals the right to access personal data (as defined in the DPA). The British

---

Singapore (16 May 2014) <https://www.pdpc.gov.sg/docs/default-source/annual-seminar-2014-pr/closing-note-for-nbsp-the-public-consultation-on-the-proposed-regulations-nbsp-.pdf?sfvrsn=0> (accessed 24 April 2015) at para 4.8.

18 This factor has also been considered relevant in determining if a request for access is frivolous or vexatious. See para 23 below.

19 *Management Corporation Strata Title Plan No 2956* [2017] PDP Digest 238 at [8].

20 c 29.

21 See s 8(2)(a) of the Data Protection Act 1998 (c 29) (UK).

Information Commissioner has stated that costs associated with "retrieval" of personal data cannot constitute "effort".[22]

20 However, in *Elliott v Lloyds TSB Bank plc*[23] ("*Elliott*"), the court explicitly disagreed with the Information Commissioner.[24] Referring to the earlier case of *Ezsias v Welsh Ministers*,[25] the court found that the "disproportionate effort" exception also included costs associated with the search for data. Both judgments were referred to and followed by the High Court in *Dawson-Damer v Taylor Wessing LLP*.[26]

21 The foregoing raises the question of what the individual's interests must be to have his request acceded to. This goes back to the question of the purpose of s 21. There is no explicit provision on what constitutes the individual's interests in the PDPA. It is submitted that s 21(1) should be clarified that the right to access is to enable the individual to:

> (a) determine the personal data in the possession or under the control of the organisation so that he can correct it if it is not accurate; or
>
> (b) know what and how his personal data is being used and to whom it may have been disclosed.

22 If the requests do not relate to these two purposes, the organisation should not bear the burden of giving the access. This will provide a measure of certainty for organisations in making the decision whether or not to accede to the request.

B. The Frivolous or Vexatious Exception

23 Paragraph 15.24 of the PDPC's *Advisory Guidelines on Key Concepts in the PDPA*[27] ("Advisory Guidelines") provides an example of what it would consider a frivolous or vexatious request. In that example, the individual

22 *Elliott v Lloyds TSB Bank plc* [2012] EW Misc 7 (CC) (24 April 2012) at [16]–[17].

23 [2012] EW Misc 7 (CC) (24 April 2012).

24 *Elliott v Lloyds TSB Bank plc* [2012] EW Misc 7 (CC) (24 April 2012) at [16]–[17].

25 [2007] All ER (D) 65.

26 [2016] 1 WLR 28; [2015] EWHC 2366 (Ch).

27 Revised on 15 July 2016.

making the request soon after the individual provided the personal data clearly had full knowledge of the information that he was requesting. Such requests would be considered frivolous or vexatious unless the individual can show otherwise. Nevertheless, not all requests are so clear cut.

24 As stated earlier, the PDPA does not require the requester to state the purpose for his request for access. Therefore, even if the requester does not state the purpose, the organisation is obliged to grant access unless it can rely on the exceptions or exemptions under the PDPA.[28]

25 It was submitted earlier that the purpose for the request should be a relevant consideration in deciding if a request is unreasonable to the organisation or disproportionate to the individual's interest. This must be correct since the purpose of a request must be a relevant factor in determining what the individual's interest is.

26 It is further submitted that the purpose of a requester should also be a relevant consideration in determining if the request is frivolous or vexatious. A distinction was drawn between the *request* and the *requester*, by the New Zealand Privacy Commissioner. It was stated that since the provision in the New Zealand Privacy Act 1993 refers to the request, an organisation cannot withhold information even if "a requester is an annoying or even malicious individual".[29] However, although there are no definitions of "frivolous" or "vexatious" in the PDPA and there are no Singapore cases addressing this point in the context of the PDPA, the guidance from the

28 As a matter of practicality, the organisation should first determine if the personal data requested is that of the requester. There should be no circumstance in which an organisation should need to provide information or personal data that does not relate to the individual.

29 Privacy Commissioner, *Vexatious, Frivolous, Trivial* <https://privacy.org.nz/the-privacy-act-and-codes/privacy-principles/access/vexatious-frivolous-trivial/> (accessed 27 March 2017). It is submitted that such fine distinctions may not be helpful in our Singaporean context where the Personal Data Protection Act 2012 (Act 26 of 2012) applies to the whole spectrum of organisations that are diverse in size and working language, and would make compliance with the Act even more difficult. A principle-based approach will be more appropriate.

PDPC in para 15.24 of the Advisory Guidelines suggests that the conduct of the requester is relevant.[30]

27 Indeed, in Hong Kong, the Administrative Appeals Board ("AAB"), which reviews appeals against the decisions of the Privacy Commissioner, had a chance to consider various cases under s 39(2)(c) of the Personal Data (Privacy) Ordinance[31] ("PDPO"), which empowers the Privacy Commissioner to decline investigating a complaint that is "frivolous or vexatious or made in bad faith". In those cases,[32] the findings all turned on the facts of the cases. Amongst the facts taken into account by the Board were the conduct and the motives of the requester. For example, in *Administrative Appeal No 16 of 2012*, the AAB found that the appeal was vexatious after examining the documentary evidence, which pointed to "the Appellant … launching a personal vendetta against the Company … She was maliciously using this Appeal to tarnish the image of those who incurred her disliking".[33]

28 In New Zealand, the equivalent to para 1(*j*)(v) of the Fifth Schedule to the PDPA is s 29(1)(j) of New Zealand's Privacy Act 1993. The New Zealand Privacy Commissioner has framed a legal test for the equivalent provision as such: "Is the requester only making the request to cause trouble, or might there be a genuine reason for the request?"[34] In this respect, the position is not unlike the position of the AAB in Hong Kong.

29 An issue that may arise in an organisation attempting to rely on this exception is where the requester has mixed motives, *ie*, where he may have a valid reason for the request in addition to other motives. In *Elliott*, the

30 The terms "frivolous" and "vexatious" are referred to in the Rules of Court (Cap 322, R 5, 2014 Rev Ed) and in cases relating to abuse of process.

31 Cap 486.

32 Administrative Appeals Board Case No 2001A11 of 2001. See also Administrative Appeal No 16 of 2012 and Administrative Appeals Board Case No 2012A14 of 2012.

33 Administrative Appeal No 16 of 2012 at [34].

34 Privacy Commissioner, *Vexatious, Frivolous, Trivial* <https://privacy.org.nz/the-privacy-act-and-codes/privacy-principles/access/vexatious-frivolous-trivial/> (accessed 27 March 2017). In *Privacy Commissioner Case Note 18109*, the Privacy Commissioner attempted to draw distinctions between a requester "patently abusing the rights of access to information, [as opposed to] exercising those rights in a bona fide manner".

Leeds County Court explored whether to exercise its statutory discretion to refuse access because the requester allegedly had a collateral purpose of using an access request to "fish" for information for a lawsuit. In doing so, it held that it was not "necessary for [the requester] to establish a lawful purpose as 'the dominant purpose' … [the test is] whether but for the collateral purpose, the claim would not have been brought at all".[35] Applying the "but for" test to the facts, the court found the requester to be honest and was "not satisfied that but for any other purpose this application would not have been brought at all".[36] It is submitted that such a positon would be consistent with the legislative intent of the PDPA and in particular the right to access under s 21(1). Therefore, if the requester has an honest motive to access his personal data, notwithstanding the "additional" motive, the organisation should not be able to deny the request under this Frivolous or Vexatious Exception.

30 Another issue is whether the organisation may deny a request on this ground where it is clear that the requester is making the request solely as an alternative to pre-action discovery or litigation discovery. Whilst such requests would be frowned upon in the UK, the New Zealand Law Commission has described access requests by individuals for official information concerning themselves, being used as an alternative to discovery under an equivalent provision in the Official Information Act 1982,[37] as "long, and judicially sanctioned, practice".[38] It appears that there is no consensus amongst courts in different jurisdictions as to whether the access rights under similar data protection statutes may be exercised for collateral or mixed purposes. This is not surprising since different jurisdictions have different rules on discovery and those rules have probably been developed in the context of different legal and statutory regimes. In Singapore's context, it may be argued that in the light of s 4(6) of the PDPA, civil and criminal discovery rules will take precedence over the PDPA access rights if the true purpose is to obtain discovery for proceedings and a request for personal data as an alternative to discovery or

35 *Elliott v Lloyds TSB Bank plc* [2012] EW Misc 7 (CC) (24 April 2012) at [83].

36 *Elliott v Lloyds TSB Bank plc* [2012] EW Misc 7 (CC) (24 April 2012) at [87].

37 Singapore does not have an equivalent Official Information Act.

38 New Zealand Law Commission, *The Public's Right to Know: Review of the Official Information Legislation* Report No 125 at paras 7.72–7.73 in the context of New Zealand's Official Information Act 1982.

pre-discovery actions should not be allowed under the PDPA in the first place. Such requests should therefore be considered "frivolous" or "vexatious" and are an abuse of process.

31 Unfortunately, such enquires are often time-consuming and costly if the organisation wishes to rely on the Frivolous or Vexatious Exception. If it is not the intent of Parliament to require organisations to be concerned with civil or criminal procedure rules in considering a request for access by an individual, then s 21(1) should be amended to explicitly prohibit the individual from making a request for such purposes.

IV. What can organisations do?

32 An organisation should prepare a form for a requester to complete for purposes of s 21 and s 22 requests. The PDPC has provided a sample form for organisations to adopt in its *Guide to Handling Access Requests*.[39] Organisations should consider adapting the form for the individual to provide information relating to the purpose for which the request is being made to assist the organisation and expedite the process. The reality is that if the request does not adversely affect the organisation's interest and if the costs of acceding to the request are not unreasonable, the organisation will as a matter of course accede to the request. If the request relates to third-party personal data, the requester should not be entitled to make the request in the first place.

33 Unfortunately, based on the current provisions in the PDPA, relying on the Disproportionate and Unreasonable Exception or the Frivolous or Vexatious Exception is not always so straightforward and can be time-consuming and costly.

V. Conclusion

34 The current provisions can lead to "abuse" by individuals using the right of access for purposes related to other ulterior motives. It is submitted that an explicit statement in s 21 as to the intent or purpose of that right will ameliorate much of the current uncertainty for both the organisations and the individuals seeking to protect the integrity of their personal data.

39 9 June 2016.

However, where the individual seeks protection of his personal data, even where there are mixed motives, the organisation should be required to provide access subject to the exceptions or prohibitions under the PDPA.

35 Of course, it can be argued that the individual may falsely declare his intention for making the request.[40] Notwithstanding this, where the principle for giving the right to request is clearly set out in legislation, that would deter requests for access for purposes that are clearly not intended by the PDPA, thereby reducing the burden of organisations.

---

40 This can be resolved by providing for a penalty and sanctions for making false declarations.

DATA ANALYTICS: CONSIDERATIONS WHEN REPURPOSING TRANSACTIONAL PERSONAL DATA UNDER THE PERSONAL DATA PROTECTION ACT*

LIM Jeffrey, Sui Yin†
LLB (National University of Singapore); Advocate and Solicitor (Singapore), Barrister-at-law (England & Wales)

LEE Yue Lin‡
LLB (King's College London); Advocate and Solicitor (Singapore)

I. Introduction

1 Rapid technological advancements have been made in data analytics, resulting in increasing sophistication in data usage, driven by a demand for better intelligence and innovation across nearly all industries.

2 Personal data is not always used for data analytics, but when it is, it can be essential. For example, an airport studying the rates at which aeroplanes take off at a terminal may not use personal data at all. By contrast, if that same airport wanted to study how quickly individuals move from check-in, to passport control, and on to boarding gates by

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Partner, WongPartnership LLP. Jeffrey's main areas of practice are in contentious and non-contentious intellectual property issues in the area of media, telecommunications, information technology, cybersecurity and data protection law. He is currently the Chairman of the Law Society's Project Law Help, the Vice Chair of the Law Society's Cybersecurity and Forensics Committee, as well as member of the Singapore Domain Name Dispute Resolution Policy Panel, the Singapore Academy of Law's Legal Technology Cluster Committee, the Law Society's Intellectual Property Committee and the Law Society's Information Technology Committee.

‡ Senior associate, WongPartnership LLP. Yue Lin's main areas of practice are in intellectual property, media, telecommunications, information technology, cybersecurity and data protection law.

tracking data from boarding passes or passports, the use of personal data is essential.

3 The use of personal data for such purposes, however, is now regulated by the Personal Data Protection Act 2012[1] ("PDPA"). In particular, organisations must address obligations under the PDPA to (a) notify individuals of the purposes for which it will collect, use or disclose personal data; and (b) obtain the consent of these individuals to such purposes, unless exceptions from consent apply.

4 The need for consent and notification brings two aspects to the fore.

5 Firstly, organisations which did not have collateral uses in mind at the point that consents were obtained may need to obtain fresh consents if they were now to repurpose that data. Securing fresh consents may be difficult where the opportunities to do so have lapsed.

6 Secondly, organisations that do anticipate what collateral uses will be needed may not be able to demand or insist on consents for these collateral uses being given, since such collateral purposes may not necessarily be required in order for the organisation to provide a product or service to that individual.

7 How then does the PDPA address these concerns and what takeaways are key?

8 In this article, we consider how organisations conduct data analytics within the realm of the PDPA, the research-specific exception from consent available under the PDPA and some of the key nuances involved in its application, and how data analytics seems to be divided into two broad aspects: (a) for researching and developing new products and services ("Innovation Research"); and (b) for quality assurance and improving products and services ("Product and Service Improvement").

A. Data analytics before the Personal Data Protection Act

9 It may help to first have context.

10 Before the PDPA, the collection, use, disclosure and processing of personal data in Singapore was not regulated by any general, overarching

1 Act 26 of 2012.

legislation although there was sector-specific legislation (*eg*, the Banking Act[2]). Sector-specific legislation aside, organisations were generally free to collect, use, disclose, process and study personal data for Innovation Research and Product and Service Improvement without having regard to issues of consent or whether the individuals were aware that data analytics were being carried out on their personal data.

11 Even where organisations did obtain consent, they could obtain wide-ranging and broad consents for as many purposes as possible, without regard to the reasonableness of imposing such consents as conditions for providing services or products.

B. Data Analytics after the Personal Data Protection Act: The "Necessity" threshold

12 Enter the PDPA. With the PDPA, organisations are now required to, among other things: (a) notify individuals of the purposes for which they collect, use or disclose their personal data; and (b) obtain their consent for such purposes *before* data is applied to such purposes (unless statutory exceptions apply).

13 In addition, in line with the general concept of reasonableness which is enshrined within the PDPA,[3] organisations can no longer seek broad, wide-ranging consents from individuals for *all* the purposes for which an organisation might want to process the collected personal data. The purposes for which consent is sought must be tied to purposes which are "reasonable".[4] Furthermore, an organisation cannot, as a condition of providing a product or service, require individuals to consent to the collection, use or disclosure of their personal data beyond "what is reasonable to provide the product or service to that individual".[5]

14 Some purposes are clearly "reasonable" in the context of the provision of a product or service and an organisation may require consent for such

2 Cap 19, 2008 Rev Ed.
3 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(1).
4 Personal Data Protection Act 2012 (Act 26 of 2012) s 18.
5 Personal Data Protection Act 2012 (Act 26 of 2012) s 14(2)(*a*).

purposes as a condition for providing the product or service.[6] However, other purposes may not necessarily be considered "reasonable" in the context of providing a product or service and would therefore be considered "optional" purposes under the PDPA.[7] For such purposes, the organisation should obtain separate notified consents from the individuals concerned, and the individuals should be allowed to withdraw their consent without concurrently having to withdraw their consent for the "required" purposes.[8]

15 Whether data analytics as a purpose is a "required" purpose for the provision of the product or service or an "optional" purpose is not always certain.

16 On the one hand, data analytics may be required as part of regular Product and Service Improvement.

17 Indeed, guidelines issued by the Personal Data Protection Commission ("PDPC") state that insofar as "the purpose of the analytics and research falls within the original purpose for which consent was given",[9] an organisation may rely on the consent previously given by the individual for a particular purpose, even where this purpose did not expressly cover research and analytics. Examples of this, as provided by the PDPC, include a telecommunications service provider analysing personal data in order to manage its network and carry out short-term planning enhancements to

6 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) para 12.20.

7 One common example of an optional purpose would include use of the personal data to send the individual marketing material on other products/services. Depending on the context, an organisation would still be able to provide the product or service even if it could not market other products or services to that individual. See also paras 7 and 8 of the Personal Data Protection Commission, *Advisory Guidelines on Requiring Consent for Marketing Purposes* (revised on 8 May 2015).

8 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) para 12.43(c).

9 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised on 28 March 2017) para 2.3.

improve the quality of mobile services provided to the individual,[10] and a business's review of its internal processes for quality assurance.[11]

18 Playing the devil's advocate, it could on the other hand also be argued that the carrying out of analytics and research is not necessarily "required" by the organisation to provide a product or service to that individual. In other words, it would still be possible for an organisation to provide a product or service without conducting any kind of analytics and research, whether such analytics relates to Innovation Research or Product and Service Improvement.

19 The "necessity" of the analytics purpose may therefore raise nice questions that turn, in each case, on the specific context and circumstances.

C. "Original purpose" restriction and Research Exception

20 Taking the PDPC's guidance into consideration, the PDPA requires an organisation looking to use personal data for research purposes to obtain the consent of the individual *unless* such research purposes fall within the ambit of the "original purpose" for which the individual's consent was given.

21 However, it may not always be clear whether this is so, or whether, in fact, the research is a new purpose for which fresh/separate consent would need to be obtained.

22 If the analytical objective of the research purpose is not within the ambit of the "original purpose" for which consent was given, or cannot be categorised as Product and Service Improvement, there may be practical difficulties to now attempt to obtain a fresh consent. The volume of individuals involved, the resource requirements and the availability of contact data for use (and how current that data is) can vary.

23 Interestingly, the PDPA appears to have anticipated this need for research by providing for a research-specific exception under the PDPA pursuant to which an organisation can collect, use or disclose personal data

10 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised on 28 March 2017) para 2.4.

11 Personal Data Protection Commission, *Advisory Guidelines for the Healthcare Sector* (revised on 28 March 2017) para 2.7.

for research purposes[12] ("Research Exception"). The Research Exception states that an organisation may collect, use or disclose personal data for "a research purpose, including historical or statistical research" if certain conditions are met, including:

(a) the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;
(b) it is impracticable for the organisation to seek the consent of the individual for the use;
(c) the personal data will not be used to contact persons to ask them to participate in the research; and
(d) linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest.

24 Limb (a) of the Research Exception requires organisations to consider whether personal data can be dispensed with for the purposes of carrying out the research, whilst limb (b) requires assessment of the practicalities of executing a consent collection exercise.

25 Whether personal data can be dispensed with and whether collecting consent is practical or impractical will likely depend on the circumstances in each case.

II. Difficulties of conducting data analytics within the Personal Data Protection Act

A. Difficulties of coming within the Research Exception

26 How easy is it then, for organisations to invoke the Research Exception? We turn to look at some issues.

12 The exceptions under the Third Schedule, para 1(*i*) read with para 2; the Fourth Schedule, para 1(*q*) read with para 4; and the Second Schedule, para 1(*r*) read with Fourth Schedule, para 1(*q*), of the Personal Data Protection Act 2012 (Act 26 of 2012).

(1) The research purpose cannot reasonably be accomplished unless personal data is provided in an individually identifiable form – "preview/access conundrum"

27 The first limb of the Research Exception provides that the organisation must be able to show that the research purpose cannot be reasonably accomplished unless the personal data is provided in an individually identifiable form.

28 Whilst the ability to satisfy this limb would depend on the circumstances, an interesting conundrum could arise where it is not even possible to determine whether personal data is necessary for the research purpose, without first sampling the personal data itself.

29 In other words, to even determine whether this first limb of the Research Exception applies, the organisation may need to access the personal data in its individually identifiable form *first* to review and consider the personal data which is available to the organisation for the proposed study before assessing whether the use of data in its individually identifiable form can be dispensed with, and even which data sets are relevant for the study.

30 Hence, if the organisation had never obtained the notified consent of these individuals for Innovative Research, the organisation seeking to rely on the Research Exception would now need to sample the personal data to consider if the Research Exception is available. However, given the lack of notified consents, the organisation will now face the awkward result of being unable to make the assessment as to the application of the Research Exception at all.

31 Indeed, it should be noted that research projects/parameters are often designed or scoped by first sampling data. Notably, certain legislative solutions to a similar problem in other jurisdictions to address this conundrum do exist.[13]

13 See paras 51–62 below for the discussion on the US Department of Health and Human Services' Standards for Privacy of Individually Identifiable Health Information on "preparatory" research, and the discussion as to s 33(2) of the Data Protection Act 1998 (c 29) (UK).

(2) When it will be considered "impracticable" for the organisation to seek consent of individuals for collection, use and disclosure of their personal data for research

32 The second limb of the Research Exception provides that in order for the research to come within the Research Exception, it must be "impracticable" for the organisation to seek the consent of the individuals for the collection, use and disclosure of their personal data for research.

33 This presents its own set of considerations.

34 From one perspective, a database is more valuable if it covers more individuals – *eg*, accuracy increases with sample size. However, if the sample size needed, and the database from which it is drawn is very large, obtaining the consents of the relevant individuals may be difficult, if not impossible, for the organisation.

35 In some cases, the relevant database from which the sample is drawn may be so large and voluminous that, even assuming consent can be obtained from each individual for Innovative Research, the consent collection exercise would take too long or consume too many resources such that it would no longer be feasible for the organisation to carry out the study.

36 Other complications include the possibility that the research objective is defeated because the sample size of individuals who consented is too small, or the sample is skewed because only a certain class of individuals generally consented.

37 The lack of a definition of "impracticability" under the PDPA has been mitigated somewhat by practical guidance which has been issued by the PDPC as to the relevant factors to consider when assessing impracticability.[14] The practical guidance provides organisations with a high level indication of what the PDPC would consider relevant in assessing whether it would be "impracticable" to seek consent.[15] Such guidelines are

14 Personal Data Protection Commission, *Practical Guidance to Queries by Medical Research Institution* <https://www.pdpc.gov.sg/docs/default-source/informal-guidance/2016-07-medical-research-institution-pg0bc83bc8844062038829ff0000d98b0f.pdf?sfvrsn=0> (accessed 24 April 2017).

15 Personal Data Protection Commission, *Practical Guidance to Queries by Medical Research Institution* <https://www.pdpc.gov.sg/docs/default-source/

(*continued on next page*)

no doubt helpful to organisations. However, given the general nature of such guidance, ultimately organisations will still have to consider for themselves the internal guidelines and standards for establishing the point at which the organisation would consider it "impracticable" to seek consent, having regard to factors such as the target population required for meaningful conclusions to be drawn from the research, the quantum of the research grant and the period allotted for the research as a condition of the research grant, *etc*. The fact-specific nature of the factors stated in the practical guidance also suggests that, unfortunately, the assessment of what would be considered "impracticable" will be a situation-specific consideration in each case. It is hoped that further development in thinking in this area will continue with, perhaps, guidelines that address the nuances discussed here.

B. Anonymisation – A means of resolving these issues?

38 One way of resolving the data protection difficulties faced by organisations in carrying out Innovative Research is to anonymise the personal data and use only de-identified data for the Innovative Research. Personal data which has been anonymised such that it cannot identify the individual would no longer be considered "personal data" and would not be regulated under the PDPA.

39 However, given the broad and inclusive definition of "personal data" under the PDPA,[16] it will generally not be sufficient to only de-identify the specific copy of the data which is being used by the organisation for that research study, especially if the de-identified copy of the data set can be easily converted back to personal data based on "other information to which the organisation *has or is likely to have access*" [emphasis added].

40 In other words, if the organisation is able to access any other information under its control or in its possession that is able to re-identify

---

informal-guidance/2016-07-medical-research-institution-pg0bc83bc8844062038829ff0000d98b0f.pdf?sfvrsn=0> (accessed 24 April 2017) para 3.

16 "Personal data" is defined in s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) as "data, whether true or not, about an individual who can be identified (*a*) from that data; or (*b*) from that data and other information to which the organisation has or is likely to have access".

the personal data, the data set would still be considered "personal data", and the PDPA would continue to apply to the treatment of this personal data.

41 It would appear, therefore, that if an organisation wants to use anonymised data for its research study, it will need to establish "effective barriers" to ensure that the anonymised data set *stays* anonymised and that the risks as to re-identification of the dataset are extremely low. Formal and informal guidance has been issued by the PDPC on the topic of anonymisation.[17]

42 Having regard to the difficulties of anonymisation, the PDPC has (recently) provided some guidance on, among other things, how organisations should assess and manage the risks of re-identification of anonymised data. It is useful to note that the PDPC has stated that it would consider an organisation to have anonymised data if "there is no serious possibility that a data user or recipient would be able to identify any individuals from the data".[18]

43 Some factors to take into account when considering whether there is a "serious possibility" that a data user or recipient of anonymised data would be able to re-identify any individuals from that data include, for example, the nature of the use of the personal data and the extent of the disclosure (*eg*, the more limited the number of individuals accessing the personal data, the better the re-identification risks can be managed), whether it is likely that the anonymised data set which is being published can be combined with other publicly available information to re-identify the individuals (*eg*, the risks of disclosure to a single entity as compared to the publication of a data set would differ), and whether the organisation intends to disclose multiple anonymised data sets (*eg*, the more data sets are disclosed, the more

17 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017); Personal Data Protection Commission, *Practical Guidance to Queries by Medical Research Institution* <https://www.pdpc.gov.sg/docs/default-source/informal-guidance/2016-07-medical-research-institution-pg0bc83bc8844062038829ff0000d98b0f.pdf?sfvrsn=0> (accessed 24 April 2017).

18 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) para 3.29.

likely it will be that the disclosed data sets can be recombined to re-identify individuals).

44 Perceptively, the PDPC has discussed the possibility that an individual could be re-identified from an anonymised data set if it is combined with public or "personal" knowledge,[19] and this should alert one to the fact that anonymisation is as much about the recipient of the anonymised data, and his resources,[20] as well as the data subject who is being de-identified. Indeed, recipients (whether they are internal recipients in intra-organisation disclosures or third-party recipients in ex-organisation disclosures) who are well resourced (or have access to other data), could well render the most well-intentioned anonymisation moot.

45 Indeed, one aspect of "big data" analytics is that, with sufficient data sets and improved computing power and techniques, it may become possible to reach a state of "near-identification" (to coin a term), *ie*, where a particular individual can be identified by his activities and transactions with certainty even if the final piece of the data sets which ultimately identify that individual by name or a unique identifier is not available, and here, the PDPC has acknowledged the "likelihood of re-identification … is likely to increase over time" as analytics capabilities evolve and circumstances change.[21]

46 For this reason, the "barriers" which the PDPC proposes that an organisation can implement to manage the risks of re-identification are necessarily diverse, ranging from legal barriers to organisational structures to technical and physical measures (*eg*, having a different department hold onto the decryption key and implementing access controls within an organisation to prevent data users from gaining access to the key, as well as making unauthorised attempts by employees or the data users or data

19 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) paras 3.17 and 3.18.

20 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) paras 3.21–3.23.

21 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) para 3.24; see also para 3.25 where assessments of risks must be necessarily made "in relation to the current state of technology".

recipients to re-identify anonymised data sets a breach of the terms of their contracts with the disclosing organisation).[22]

47 The recent guidelines issued by the PDPC provide useful guidance on how an organisation may (a) disclose anonymised data between departments in the same organisation; and (b) disclose anonymised data to other parties outside the organisation.

48 However, given the fluidity of data flows and the variety of data sources which organisations have nowadays, the implementation of effective policies segregating anonymised data from the rest of the organisation could, in practical terms, be difficult to implement.

49 Furthermore, if the organisation requires individually identifiable data at the outset in order to determine the eligibility of the study before even commencing on the research study, anonymisation may not necessarily be a method that is open to them for the purposes of working around the consent requirements of the PDPA.

50 This is to say nothing of the logistical challenges to attempt anonymisation if the database is comprised of historical records stretching back years, in disparate or fragmented databases or in partially-manual form, or partially electronic form in diverse systems.

III. How research is handled in other jurisdictions

51 Though the underlying legal framework (and even legal philosophy underpinning it) may differ, it may be useful to consider how some of these issues are addressed in other jurisdictions.

A. The US framework

52 In the US, the general rule is for the organisation to obtain authorisation from the relevant individuals for research use or disclosure of their protected health information ("PHI"), although there is a specific exception for activities which are "preparatory to research".

22 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) para 3.39.

53 Under this exception, covered entities (a covered entity includes healthcare providers which electronically transmit health information in connection with certain transactions such as claims and benefit eligibility inquiries and referral authorisation requests, *etc*) may permit researchers to review PHI contained in medical records or elsewhere to prepare a research protocol, or for similar purposes preparatory to research, provided certain requirements are met.[23]

54 The fact that a specific carve-out is provided for activities "preparatory to research" under the Standards for Privacy of Individually Identifiable Health Information (issued to implement the requirement of the US Health Insurance Portability and Accountability Act 1996) seems to suggest that overseas, at least, the conceptual difficulties of ascertaining whether an exception from consent is applicable for the use of personal data for research, without being able to access the personal data records, are acknowledged.

55 Importantly, this exception allows a researcher to determine, for example, whether a sufficient number or type of records exists to conduct the research, thus going some way in resolving some of the conceptual issues which were raised above in respect of the application of the Research Exception.

B. The UK framework

56 The UK Data Protection Act 1998[24] ("DPA") provides for a specific carve-out from the requirement to obtain consent (as well as a number of other data processing principles under the DPA) where personal data is processed for research purposes.

23 The researcher will not remove any protected health information from the covered entity, and the researcher must provide the covered entity with representations that the protected health information for which access is sought is necessary for the research purpose (see 45 CFR 164.512(i)(1)(ii) of the US Department of Health and Human Services' Standards for Privacy of Individually Identifiable Health Information).

24 c 29.

57 The conditions to be met by an organisation or individual before processing the personal data for research purposes are, however, quite different from the conditions imposed under the Research Exception.

58 A "research purpose" for the purposes of the DPA "includes statistical or historical purposes",[25] a definition that is not unlike the language in the Research Exception.

59 There are two primary conditions (the "relevant conditions" for the purposes of s 33 of the DPA) which need to be satisfied before personal data can be processed for research purposes, namely:[26]

(a) that the data are not processed to support measures or decisions with respect to particular individuals, and

(b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

60 Importantly for organisations which wish to use personal data for research, the exemption is also applicable to data where the collection of the personal data for research is *only a secondary purpose*,[27] assuming all the conditions under s 33 of the DPA are met.

61 It would appear that the DPA takes an even more robust position in respect of the conducting of research as compared to the US.

62 This suggests that in other jurisdictions, perhaps, the increasing importance of all types of research and data analytics beyond the conducting of research for the narrow scope of Product and Service Improvement was considered and recognised when their data protection legislation was effected.

---

25 Data Protection Act 1998 (c 29) (UK) s 33.

26 Data Protection Act 1998 (c 29) (UK) s 33(1).

27 See s 33(2) of the Data Protection Act 1998 (c 29) (UK), which provides that, for the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

The "second data protection principle" of the Data Protection Act 1998 states as follows: "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."

IV. Conclusion

63 The data protection landscape in Singapore is still relatively young compared to some of the more mature data protection regimes overseas.

64 However, given the importance of data analytics and research in business as well as the vast amounts of personal data which we are generating these days, it may be useful to also take into consideration the current practices of businesses when issuing guidance on the data protection legislation. A fine balance needs to be struck between protecting the rights of individuals in relation to their personal data and the need of organisations to collect, use and disclose personal data.

ROLE OF AUDIT IN YOUR ORGANISATION'S PERSONAL DATA PROTECTION ACT 2012 COMPLIANCE PROGRAMME*

AWAT Sheela†
Advocate and Solicitor (Singapore), Solicitor (England & Wales)

1 Now that you have understood the requirements of the Personal Data Protection Act 2012[1] ("PDPA"), reviewed your organisation's collection, use and disclosure of personal data of employees and customers, put in place policies and processes to ensure your organisation complies with all its obligations under the Act, trained your staff on the policies and procedures and amended your contracts to ensure the necessary legal provisions have been incorporated in the relevant contracts to protect your organisation, you may give yourself a pat on your back for a job well done.

2 Is this all or is there something more that needs to be done? Yes, something more needs to be done, failing which your organisation may be open to risks it may not even be aware of. To ensure the necessary degree of confidence in its PDPA compliance programme, an organisation should conduct a periodic audit.

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of her employer. All errors remain the author's own.

† Sheela has 25 years' legal expertise gained at two international law firms and being part of the Asia-Pacific senior management team for two global multinationals – a Fortune 500 group listed in New York and another listed in London in her roles as Vice-President and Head of Legal, including extensive experience in implementing compliance programs. Her current legal practice at AT Law Practice LLP includes advising multinational corporation and small and medium-sized enterprises on their Personal Data Protection Act compliance program, its implementation and audit.

1 Act 26 of 2012.

I. Why audit?

3 According to the Institute of Internal Auditors' ("IIA") International Professional Practices Framework,[2] internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

4 You would be familiar with the concept of larger organisations already having an audit process in place for its financial statements, the purpose of which is to ensure the necessary degree of confidence which is achieved by the auditors furnishing an opinion that the financial statements are prepared, in all material respects, in accordance with the applicable financial reporting framework.

5 Similarly, when any new law comes into force requiring compliance for some legal matters, for example, anti-trust laws, anti-bribery laws and personal data protection laws, a compliance programme must be implemented.

6 It is important to appreciate that there are consequences, sometimes severe, for failing to comply with the law and often it is lack of understanding of what is required by the law that exposes organisations to far greater risks than necessary, when a lot, if not most, of the compliance obligations can be easily satisfied. Thus, conducting an audit ensures a systematic and disciplined approach to risk management.

II. Role of audit in a legal compliance life-cycle

7 Auditing for legal compliance is a process to review an organisation's operations and its compliance with the relevant laws and other applicable guidelines. You need to audit to take stock of where your organisation is at in complying with its obligations relating to personal data protection under the PDPA and its related regulations within the framework of the advisory guidelines issued by the Personal Data Protection Commission ("PDPC").

---

2 <http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search%C2%Bcdefinition> (accessed 24 April 2017).

8 A well conducted audit helps an organisation mitigate risk of sanctions for non-compliance and reputational risk if found not to be complying with the law. The following paragraphs will briefly touch on some of the sanctions under the PDPA.

9 Sanctions for non-compliance under the PDPA are wide-reaching and include financial penalties where the PDPC has the power to impose fines of up to $1m for breach of the PDPA's data protection provisions (*ie*, Pts III–VI of the PDPA). In addition, breach of the PDPA's "Do Not Call" provisions (in Pt IX of the PDPA) is an offence carrying a fine of up to $10,000. The PDPC has the discretion to compound such offences and the PDPA also imposes personal liability on any officer of the organisation if the offence was committed with the consent or connivance of the officer or is attributable to neglect on the part of the officer. There are also additional obligations with regard to access to and correction of personal data which an organisation needs to be cognisant of. To top it all, besides criminal sanctions, an organisation may face civil action from individuals pursuant to s 32 of the PDPA.

III. Steps in the audit process

10 In dealing with the audit process, in conjunction with reviewing the organisation's policies, procedures, controls as well as evidence of compliance with its compliance programme, there are many different components of the organisation's operations that will have to be considered. Such components depend on the size of the organisation and the complexity of the organisation's operations including:

(a) the technology used within the organisation;
(b) touchpoints within the organisation of incoming personal data;
(c) how the organisation collects, uses and discloses personal data;
(d) whether the organisation uses data intermediaries; and
(e) whether there are other third-party service providers that have access to personal data, *etc*.

11 Nevertheless, the audit process, which comprises numerous phases, in essence can be summarised into the following steps:

(a) planning for audit;
(b) preparation for audit;
(c) conducting the audit;
(d) recording the audit results;

(e) reporting the compliance audit results; and
(f) follow-up.

IV. Role and competencies of a good auditor

12 Although the PDPA is applied equally to organisations, no two organisations have exactly the same operations. Thus, the audit work will have to be based on the individual organisation's operations. What amounts to adequate audit evidence is a matter of judgment of the auditors. It is therefore important to appoint skilled and experienced auditors who have a good grasp of the requirements under the law, and a good understanding of how the organisation handles personal data, including all the touchpoints in the organisation's operations which handle personal data in any way. A good auditor must be able to assess risk. The auditor must have business acumen and have the confidence in giving a clear opinion on the solutions that are likely to work and that which would be of high risk. In other words, he must take a business-centric approach to risk assessment and risk management, whilst having a good grasp of the legal requirements. It goes without saying that the auditor will have to apply integrity and objectivity as well as a dose of scepticism when evaluating the facts. Set out below are some of the basic characteristics of a good auditor. Do look for these characteristics when appointing an auditor for your compliance programme:

(a) understands the business operation;
(b) understands the requirements of the PDPA;
(c) applies professional ethics;
(d) manages the audit function;
(e) excellent communicator;
(f) collaborative; and
(g) sound judgment based on ability to think critically.

13 From the above, it is crucial to appreciate that although the main responsibility of conducting an audit lies with the auditor(s), the auditor's judgment on the facts does not only depend on the skill and expertise of the auditor, but also the participants in the audit exercise who furnish the necessary information and inputs to the auditor. For example, if an auditor is not told accurately what the marketing department does with the personal data of clients and contacts that they are targeting, then no matter how good an expert the auditor is, his judgment at best is based on the

information he is furnished by the marketing department. Thus, it is very important to ensure that where an auditor has to rely on information furnished to him by other participants in the audit process, that information is accurate and comprehensive.

14 Be prepared to find that the various stakeholders in any organisation may have differing views on the objective of an audit exercise and the quality of the audit results. The legal department head may seek a reasonably thorough audit to be secure that all the main legal risks are mitigated while the sales department head may push for minimum disruption to their sales activities and the finance department head would like audit costs to be minimal. All these considerations are valid and need to be balanced finely by facilitating the required dialogue between the key stakeholders involved in the exercise.

V. Timings of the audit

15 Now, just over two and a half years since all the provisions of the PDPA came into force, is a good time to take stock of where your organisation is at in complying with its obligations under the PDPA.

16 A one-off audit does not give an organisation the sense of comfort and security it needs about its degree of compliance with the relevant law. The organisation needs to put an infrastructure in place to conduct a periodic audit to ensure the necessary degree of confidence that its existing compliance policies and processes adequately cover the length and breadth of its operations at the relevant time as well as to ensure confidence that its people are applying those policies and processes, as laid down by the organisation, correctly and unfailingly.

VI. Internal or external audit?

17 To audit is to conduct a review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend changes in controls, policies and/or procedures, to the extent necessary to comply with your organisation's obligations under the PDPA. An internal audit may be carried out by an individual employee or a team of employees of the organisation. It may also be carried out by engaging an external consultant or more than one consultant depending on the size of the

organisation. Usually, if the organisation has an audit department, it may choose to leave this responsibility with its audit department. But pulling together a temporary team of "auditors" from the ranks of its employees to conduct an audit may not serve the purpose as it is unlikely to provide the required skills, independence, objectivity and robustness that the exercise requires.

VII. Conclusion

18 A well-executed timely audit would be able to bring to light gaps in the compliance programme that was rolled out within the organisation, such as failure on the part of the organisation to comply with any newly promulgated regulations, and human short-comings in the documentation of policies and processes relating to the relevant compliance programme as well as in the implementation of the relevant policies and processes. This would enable management to evaluate the risk(s) that have come to light and to decide whether they need to take any steps to address any one or more of the said risk(s). Sometimes, a gap or risk that has come to light is inconsequential or to address it may require a huge cost. It such a situation, management may choose to take that risk. In other situations, a small action or simple correction in a policy and or a process may mitigate a huge risk and therefore it is always prudent to remember that a stitch in time saves nine.

TWO ESSENTIAL DATA PROTECTION STRATEGIES*

Elgin KOH†
B Eng Computer Engineering (University of Canberra)

I. Introduction

1 The increasing number of reports of personal data breaches in Singapore has led to calls for organisations to step up their efforts in protecting personal data.[1] Given the increasing concern of individuals towards their personal data, there is a need for organisations to properly evaluate their strategy in approaching personal data protection. This article seeks to present two strategies that organisations can incorporate in their systems, processes and practices: (a) data protection by design and (b) data protection impact assessment.

2 The two strategies described in this article are recommended as best practices by data protection authorities worldwide, and should be considered essential to an organisation's data protection efforts.

II. Data protection by design

3 The strategy of data protection by design ("DPD"), also referred to as privacy by design, puts data protection at the heart of a business process, product, service or information technology ("IT") system's design. Applying this strategy requires organisations to adopt a ground-up approach by considering and embedding data protection at every step of the design process.

4 Although implementing DPD may potentially add to the initial setup effort and cost of a project (and even an increase in manpower), the benefits of implementing such a system will, in the author's view, pay off in the long

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of her employer. All errors remain the author's own.

† Manager, Operations, Personal Data Protection Commission.

1 For example, see Irene Tham, "Time to Step up Efforts to Ensure Security of Personal Information" *The Straits Times* (1 February 2017).

term. Besides being a means by which organisations can seek to achieve compliance with data protection legislation, the benefits of having DPD include:

(a) early identification and mitigation of data protection risks;

(b) enhanced trust placed in the organisation by individuals;

(c) effective data protection measures that work seamlessly with the organisation's business and do not impair business operations;

(d) increased awareness of data protection within the organisation; and

(e) minimising the risk of data losses and disruption in business of the organisation.

5 While there are many approaches to implementing DPD, one of the most prominent was developed by Dr Ann Cavoukian (who was the then Information and Privacy Commissioner of Ontario) in what she calls the "7 Foundational Principles of Privacy by Design"[2] ("Principles"). The objectives of the Principles are to ensure the protection of personal data by organisations, while at the same time allowing individuals to have control over their personal data.

6 These Principles are intended to be a high-level guide, and organisations should use them as a basis for making their own decisions on the data protection measures to include in their designs. The table below describes the Principles, and along with that, sets out how these principles may be translated into examples/data protection methods in practice.

2 Ann Cavoukian, PhD, Information and Privacy Commissioner of Ontario, Canada, "Privacy by Design – The 7 Foundational Principles" (revised January 2011) <http://ipc.on.ca/wp-content/uploads/Resources/7foundational principles.pdf> (accessed 15 May 2017).

No	Principle	Possible Methods
1	**Proactive not Reactive; Preventative not Remedial** *Anticipate and prevent privacy risks from occurring.*	Conduct risk assessments to identify possible privacy risks, and then implement measures to mitigate these risks. An example of a privacy risk is excessive collection – the collection of personal data beyond what is necessary for the business process.
2	**Privacy as the Default Setting** *Personal data is protected without action from the individual.*	In obtaining consent for the collection, use or disclosure of personal data, users should be required to perform an explicit action to indicate their consent, for example by clicking on a checkbox.
3	**Privacy Embedded into Design** *Privacy is a key requirement, and not added on as an afterthought.*	Pseudonymise (obscure) personal data when performing data analysis. For example, an organisation analysing the shopping habits of consumers will not need to know the names and contact details of each individual consumer. Such personal data can be replaced by a unique identifier.
4	**Full Functionality – Positive-Sum, not Zero-Sum** *Both privacy and security can co-exist without affecting the other.*	Implementing strict access controls to video surveillance systems placed in public areas will ensure that personal data (in the form of recorded images) will be protected, while not affecting the effectiveness of these systems in enhancing public security and safety.
5	**End-to-End Security – Full Lifecycle Protection** *Secure handling of personal data through every stage of the data lifecycle, from collection to disposal.*	Database systems containing personal data should be protected with the appropriate IT security measures, *eg*, firewalls and anti-virus software. Additionally, personal data in the databases can be encrypted to prevent them being exposed in the event of a successful attack.

6	**Visibility and Transparency – Keep it Open** *All parts of the project operation and policies are open to all stakeholders.*	State clearly (*eg*, by using infographics), on the user registration form, so that users know at a glance what personal data are being collected, what they are used for, and to whom they will be disclosed.
7	**Respect for User Privacy – Keep it User Centric** *Protect the interests of the individual.*	Have a function for the individual to view and correct the personal data that have been collected by the organisation. For example, by having online user profile management.

7 The impact of DPD on the organisation is most effective when embraced by all members of the project team, which includes designers, developers and data protection officers. An organisation should therefore seek to promote DPD within the organisation itself, and to increase staff awareness. Most importantly, management needs to be convinced of the approach, so that there can be necessary oversight and directions to build in data protection directly into the technology, systems and practices of the company. In the long term, an organisation that implements DPD may reap the benefits of not just being compliant with data protection legislation or requirements, but may also gain the trust and confidence of customers whose personal data they are handling. This ultimately gives the company a sustainable competitive advantage over other companies that may not practice DPD.

8 Although DPD is intended to be implemented for new projects, it can also be adapted for existing projects, where there are existing policies and processes already put in place. For such cases, an organisation should first conduct an assessment to understand more of its processes, the way it handles personal data, and the risks to the personal data. Through such an assessment, the organisation can specifically address the risks to security of the personal data and implement data protection measures with reference to DPD.

9 One of the assessments that the organisation may conduct to examine its approach to handling personal data protection is the data protection impact assessment ("DPIA").

III. Data protection impact assessment

10 While an organisation might be tempted to focus on just implementing the most commonly-used personal data protection policies and processes, a far more effective way would be to adopt a risk management approach that enables organisations to identify and address the specific or identified risks in the organisation's system, policy and process. This would help ensure that the implemented policies and processes strike a balance between protection of personal data and operational efficiency. If an organisation implements data protection measures without first identifying the risks, they may introduce measures that are overly restrictive or cumbersome to either the customer or staff. This may lead to poor customer experiences and increased cost of operations. Above all, organisations may also introduce data protection measures that are ineffective, which would lead to wasted costs and efforts by the organisation.

11 Risk management is the practice of identifying, assessing and controlling risks. In terms of personal data protection, a risk is a potential cause of a breach of the organisation's personal data protection obligations. A risk management approach to personal data protection would thus entail:

(a) *identifying* the risks that might cause a breach;

(b) assessing each risk to determine the *likelihood* of it causing a breach;

(c) assessing each risk to determine the *impact* (to the organisation and affected individuals) of a breach caused by it; and

(d) controlling each risk by reducing its likelihood and/or impact.

12 A DPIA is a process that utilises the risk management approach, and has the function of identifying and mitigating the personal data protection risks faced by an organisation. It can be considered as a way to apply structure to risk management in data protection. The advantages of performing a DPIA include:

(a) providing management of the organisation with a better understanding of how personal data are handled within the organisation;

(b) early identification and resolution of potential personal data protection issues;

(c) avoidance of excessive personal data protection policies that hinder operations;

(d) lowering risk of breaching personal data protection laws and obligations; and

(e) clear evidence that the organisation takes responsibility for personal data protection.

13 Many data protection experts and authorities recommend that organisations conduct a DPIA on new projects, which could be in the form of a business/work process, policy, activity, procedure or IT system, that involves personal data. Organisations can also conduct DPIAs on existing projects/processes, to identify gaps in the proper handling of personal data. To be effective, DPIAs should be conducted by a team consisting of staff who are familiar with the project/process, together with staff who are familiar with the organisation's personal data protection obligations (*eg*, the data protection officer).

14 The scale and complexity of a DPIA will depend on the nature of the project or process to be assessed. However, to be comprehensive and effective, a DPIA should consist of the following steps:

(a) Compiling a data inventory of the types of personal data (*eg*, name, mobile number) collected, as well as the purposes for collecting each type of personal data. This would help organisations to ensure that only personal data essential for business operations are collected.

(b) Mapping the flow of personal data within the organisation, from collection to processing and storage. This would help organisations to identify the persons or external parties (*eg*, IT vendors) who have access to the data, or to whom the personal data is disclosed. Organisations can then use the data flow map to ensure that personnel who have access to the personal data have valid reasons for doing so.

(c) Analysing the data inventory and data flow map to identify risks, which are potential causes of personal data breaches.

(d) Assessing each risk to determine the likelihood of it causing a personal data breach, as well as the corresponding impact on the organisation and individuals, if such a breach occurred.

(e) Determining the mitigating actions to be taken for each risk. Such actions should be in the form of measures to reduce the likelihood or impact of the risk, or even changes in the organisation's operational processes to remove the risk altogether.

15 After the DPIA has been performed, the organisation should proceed to implement the mitigating actions so that the overall risk of the project is reduced. Further DPIAs should be conducted if there is a change in the way the project handles personal data, or if there is a change in the type of personal data being collected.

IV. Data protection impact assessment and the Personal Data Protection Act

16 Singapore's Personal Data Protection Act[3] ("PDPA") requires organisations to protect the personal data they collect and/or process, inform individuals why and how their personal data are used, as well as to provide individuals with a means of controlling their personal data.

17 Organisations can ensure that they comply by meeting the nine main data protection obligations of the PDPA:

(a) Consent Obligation;
(b) Purpose Limitation Obligation;
(c) Notification Obligation;
(d) Access and Correction Obligation;
(e) Accuracy Obligation;
(f) Protection Obligation;
(g) Retention Limitation Obligation;
(h) Transfer Limitation Obligation; and
(i) Openness Obligation.

18 For organisations in Singapore, a DPIA based on the PDPA can be conducted by identifying and assessing the risks that would lead to the project or process not meeting any one of the nine obligations. As an example of putting DPIA in practice (based on the obligations found in the PDPA), the table below describes some risks that may be identified by organisations as they perform their DPIA, as well as actions that could be taken to mitigate the risk.

3 Act 26 of 2012.

No	Obligation	Risk	Possible Mitigating Action
1	Consent	Sending marketing e-mails to customers who did not consent to receiving marketing e-mails.	Implement an IT system (*eg*, customer relationship management system) to ensure that consent is recorded, and that consent is checked before sending e-mails.
2	Purpose Limitation	Requiring personal data that the individual deems excessive may result in the individual choosing not to engage the organisation.	Review collection forms/web pages to verify that there are reasonable justifications for collecting each type of personal data.
3	Notification	Having a privacy policy that is difficult to read and understand will make it harder for customers to trust the organisation.	Design the privacy policy web page to include graphics and simple language, so that it is easier to understand the purposes of collecting the individual's personal data.
4	Access and Correction	Having insufficient processes for individuals to correct their data may affect the accuracy of the data.	Implement IT systems (or functions in existing systems) to allow customer-facing staff to correct a customer's data after verifying the customer's identity. At the same time, the process for correcting the personal data should be made known to customers (*eg*, by publishing on the organisation's website).
5	Accuracy	Not having a process to ensure that collected personal data are accurate may result in incorrect decisions regarding the individual.	Implement procedures to verify whether the personal data need to be updated, and if so, update the individual's personal data on a regular basis.

6	Protection	Storing personal data in an inadequately secured IT system may result in the exposure of the personal data when the system is successfully attacked.	Implement regular security testing in the form of vulnerability scanning or penetration tests to check that IT security measures are sufficient.
7	Retention Limitation	Personal data that are no longer needed are not deleted securely. This might lead to the personal data being recovered.	Use data erasure software that implements industry and government standard deletion algorithms to delete personal data from hard drives.
8	Transfer Limitation	Transferring personal data to an organisation in another country without comparable personal data protection laws may result in a data breach after the transfer as the other organisation is not obliged to protect the personal data to the same standard.	Include clauses requiring that the receiving organisation protect the personal data to a standard comparable under the PDPA.
9	Openness	Customers are unable to find out about the organisation's data protection policies, practices and complaints process.	Publish the policies and processes on the organisation's website, and have links to these pages at the places where customers would need to reference them (*eg*, customer registration page).

19 While the above is not meant to be instructive on what the processes or practices that would comply with the PDPA are, it does give a flavour as to how one may wish to approach DPIA and to align the organisation's processes and practices to comply with the PDPA. With proper implementation and execution, DPIA may well be a nifty tool for organisations to have in seeking to comply with the PDPA.

V. Data protection management programme

20 DPD and DPIAs are essential strategies for ensuring that personal data are handled properly at an individual project level. However, as

organisations grow and the number of projects increase, there will be a need to organise and manage the numerous DPD methods being implemented, as well as the many DPIAs that are being conducted.

21 Proper management of the various data protection activities at an organisational level will help to ensure that data protection strategies are applied consistently to individual projects, thus enhancing the overall level of data protection within the organisation. This can be in the form of an overarching programme (*ie*, a data protection management programme) that sets out an organisation's personal data protection concepts, policies and practices; including the policies and design patterns for applying DPD to common requirements (*eg*, collection of personal data via website), as well as processes and tools (*eg*, templates) for conducting DPIAs. The programme could also contain a depository of previously utilised DPD techniques and previously conducted DPIAs, so that lessons learned from past projects can be applied.

22 Additionally, the programme should also define the data protection governance structure in the organisation. This includes the roles and responsibilities of staff members, reporting lines, as well as controls for ensuring that data protection policies are followed. Ultimately, the programme's effectiveness will depend on how well the organisation's staff perform the various data protection activities. Staff training, together with well-designed tools and processes will thus be essential.

VI. Conclusion

21 DPD and DPIA are essential strategies that organisations should employ as part of their efforts to meet their personal data protection obligations. These strategies will help to ensure that the organisation handles personal data in a manner that minimises the risk of exposing the data, promotes trust and confidence in the organisation, and does not hinder the organisation's business operations. In order to apply these strategies effectively across multiple projects, organisations should implement a data protection programme that enables project teams to apply DPD and conduct DPIAs in an effective and repeatable manner.

INTERNATIONAL DEVELOPMENTS IN DATA PROTECTION*

Jansen AW†
LLB (National University of Singapore); Advocate and Solicitor (Singapore); CIPP/E, CIPP/A, CIPM

1 A key theme of the Personal Data Protection Act 2012[1] ("PDPA"), and indeed its stated purpose, is to govern the processing of personal data in a manner that recognises the rights of individuals to protect their personal data and the needs of organisations to process personal data for legitimate and reasonable purposes.[2] The PDPA is thus intended to achieve a balance between the needs, concerns and rights of individuals, on the one hand, and those of organisations, on the other. Although not expressly stated, the needs and concerns of society at large are also important considerations.

2 The need to balance such interests was mentioned by the (then) Minister for Information, Communications and the Arts, Assoc Prof Dr Yaacob Ibrahim during the second reading speech for the Personal Data Protection Bill[3] ("PDP Bill"):[4]

> The [PDP Bill] has been crafted to strike a balance between protecting the interests of individuals, and the need to keep compliance costs manageable for organisations … The enactment of the [PDP Bill] will strengthen Singapore's overall competitiveness, and enhance our status as a trusted hub and choice location for global data management and processing services.

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors remain the author's own.

† Assistant Chief Counsel, Personal Data Protection Commission. The author would like to thank Yeong Zee Kin and David N Alfred for their guidance and helpful comments on the article.

1 Act 26 of 2012.

2 See s 3 of the Personal Data Protection Act 2012 (Act 26 of 2012).

3 Bill No 24 of 2012.

4 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

3 This balancing approach is not unique to the PDPA. For example, the European Union's ("EU") General Data Protection Regulation[5] ("GDPR") has, as one of its core principles, the need for "fairness" and "proportionality" in the processing of personal data. As mentioned by Lee A Bygrave:[6]

> [T]he notion of fairness undoubtedly means that, in striving to achieve their data-processing goals, data controllers must take account of the interests and reasonable expectations of data subjects … [t]his means that the collection and further processing of personal data must be carried out in a manner that does not in the circumstances intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity. In other words, the notion of fairness brings with it requirements of balance and proportionality.

4 That is not to say that under the PDPA, there is always a balancing of two competing interests – those of organisations and individuals – where a tilt in favour of one side's interests necessarily means tilting away from the other. Rather, the PDPA could seek to achieve a balance that promotes *both* the individual's and organisation's interests as far as possible (especially in instances where these interests can be aligned).

5 Based on statistics collected by the Personal Data Protection Commission ("PDPC"), it appears that the PDPA has been well received and both organisations and individuals in Singapore have found it to be beneficial to their interests. In a consumer survey report produced by the PDPC in 2015,[7] it was found that 89.9% of consumers regarded the PDPA to be a good initiative, with 80.2% agreeing that they had better control over their personal data since the PDPA was introduced. In a similar survey

---

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter "GDPR").

6 Lee A Bygrave, *Data Protection law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002) at p 58.

7 Personal Data Protection Commission, *Consumer Survey on the Personal Data Protection Act September 2015* <http://www.pdpc.gov.sg/docs/default-source/Reports/pdpc-consumer-survey-report-(sept-2015).pdf?sfvrsn=2> (accessed 15 May 2017).

done on industry players,[8] it was found that organisations' sentiments towards the PDPA were generally positive; 82.3% of organisations expressed that the PDPA was beneficial in strengthening Singapore's position as a trusted hub and choice location for data hosting and data processing activities and 76.2% believed that the PDPA was beneficial for organisations.

6 Although the PDPA appears to have achieved some success in striking the appropriate balance between the various stakeholder interests, there is no place for complacency. Technology is evolving at a dizzying pace and the old ways in which data are processed are quickly replaced by the new. Data protection laws in a number of countries are presently under review and the GDPR will come into force in May 2018.

7 This article considers international developments which may provide some ideas on where the balance of various stakeholder interests under the PDPA can be strengthened or improved in relation to the following:

(a) the consent regime under the PDPA;
(b) data breach notifications; and
(c) pseudonymisation.

I. Global developments with the consent regime

A. Limitations of the consent model

8 The PDPA adopts a consent-based model which requires organisations to obtain consent from individuals in order to collect, use or disclose the individuals' personal data. This model is not unique to the PDPA and is also found in various laws which are based on the Organisation for Economic Co-operation and Development ("OECD") guidelines.

9 The PDPA also provides for certain circumstances where an organisation may collect, use or disclose personal data without the need to

8 Personal Data Protection Commission, *Industry Survey on the Personal Data Protection Act September 2015* <http://www.pdpc.gov.sg/docs/default-source/Reports/pdpc-industry-survey-report-(sept-2015).pdf?sfvrsn=2> (accessed 15 May 2017).

obtain consent.[9] However, it is not always the case that an organisation with a legitimate interest in processing personal data is able to either obtain consent or rely on an exception under the PDPA. As will be seen below, there are situations where a consent-based model may unnecessarily restrict organisations without enhancing the interests of individuals.

10 The Office of the Privacy Commissioner of Canada ("OPC") recently launched a consultation to look into the requirement for obtaining consent under Canada's national data protection law, the Personal Information Protection and Electronic Documents Act[10] ("PIPEDA"). This stems from a debate on the viability of the consent-based model in today's technological climate. In its discussion paper on the subject ("OPC Report"),[11] the OPC has identified some areas where the consent model is problematic and two, in particular, are of particular note to us.

11 First, in the area of big data and data analytics, the OPC has noted that advances in technology are opening up new data uses that makes it difficult to anticipate uses that will be made of the data later on.[12] To require a strict regime of consent on all such subsequent uses may be unduly restrictive on organisations seeking to tap into the new uses of data. Additionally, there are increasingly new ways of reconstituting identities from what was previously non-identifiable data, and new ways of extracting information about the individual from generic data.[13] The line therefore becomes blurred as to when data are considered personal data, and correspondingly when consent needs to be obtained.

12 Second, in the area of the Internet of Things ("IoT"),[14] there, too, are unique challenges presented. It is commonplace for IoT devices to require the ubiquitous collection and analysis of the user's movements or activities in order to provide the user with a customised experience. It therefore

9 Personal Data Protection Act 2012 (Act 26 of 2012) s 13.

10 SC 2000, c 5.

11 Policy and Research Group of the Office of the Privacy Commissioner of Canada, *Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent under the Personal Information Protection and Electronic Documents Act* <https://www.priv.gc.ca/media/1806/consent_201605_e.pdf> (accessed 15 May 2017) (hereinafter "OPC Report").

12 OPC Report at p 7.

13 OPC Report at p 7.

14 OPC Report at p 8.

becomes a challenge to obtain consent that covers all collection and uses of the personal data by these devices.

13 The challenge is made worse by the fact that the IoT environment is often made up of a complex (and invisible) web of devices (or things) that each collect and share data with the other devices (or things).[15] Must there be consent for the collection and use of personal data for each of these devices, and for each of their functions that involves personal data? If so, it may create difficulties for organisations to comply.

14 Additionally, in such an environment, the OPC has observed that it would be difficult to convey meaningful information about the risks to privacy in order to obtain informed consent.[16] The more complex the IoT environment, the harder it is to formulate a privacy policy which a lay user of the IoT can easily understand. And indeed, the user may not wish to read it if the user is not concerned with the internal mechanics of the system, but just the functions and features of the overall system.

15 In this regard, the traditional consent-based model appears to face increasing pressure with the development of such technologies. These limitations of the consent-based model do not just appear in areas of new technology only. For example, in a case where an ex-employee has fraudulently misrepresented his employment status and association with his former employer to customers of his former employer and the employer needs to inform its existing customers of the facts, the requirement to obtain consent may be unduly restrictive on the employer on what he can inform his customers.[17] The search for an alternative or complementary basis to the consent regime has to be technology-neutral.

B. Views from abroad

16 Given the limitations of the consent-based model regime, some overseas data protection authorities have recognised the need to look for alternatives.

15 OPC Report at p 8.

16 OPC Report at p 8.

17 *Jump Rope (Singapore)* [2016] SGPDPC 21 at [11].

17 In response to the European Commission's consultation on potential reforms to the EU's e-Privacy Directive,[18] the UK's Information Commissioner's Office ("ICO") has expressed the view that there is a case for an exemption or alternative basis for processing personal data other than consent – because it has not always delivered the expected protection of individuals in all instances of processing.[19] For example, the obtaining of the consent itself may require, paradoxically, some initial personal data to be processed, which an organisation may not seek consent for, since it may not be practical for it to do so.[20] The ICO mentioned that the rules should seek to achieve a proportionate balance between the legitimate interests of information society service providers and the privacy rights of individuals.

18 As mentioned above, the OPC has also started looking at some alternatives to consent, which include:[21]

> (a) Implementing "no-go zones" which set out the circumstances in which the collection, use or disclosure of personal data is permitted or not permitted.
>
> (b) Requiring a corresponding degree of privacy protection to be implemented depending on the risk with which data can be de-identified or re-identified.
>
> (c) Broadening permissible grounds for processing to include processing for legitimate business interests or making it a further exception to the requirement to obtain consent.

19 Additionally, the OPC has suggested enhancing the consent-based model in its national legislation by, for example, requiring greater

---

18 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).

19 *Questionnaire for the Public Consultation on the Evaluation and Review of the E-Privacy Directive* <https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1624602/eu-commission-e-privacy-directive-review-ico-submission-20160701.pdf> (accessed 15 May 2017) (hereinafter "ICO Consultation") at p 23.

20 Example arising from the Information Commissioner's Office's comments in the ICO Consultation at p 23.

21 OPC Report at pp 14–19.

transparency in privacy policies and notices or having technology-specific safeguards.

C. Legitimate interest as an established basis for collection, use or disclosure without consent

20 In considering how to address the above issues, one approach may be to allow personal data to be collected, used and disclosed without consent for certain legitimate interests. A similar approach is found in the EU's Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on Free Movement of Such Data[22] ("EU Directive") and the GDPR. Under the EU Directive, one of the lawful grounds for processing of personal data is where the processing is necessary for the purposes of the legitimate interests of the controller or a third party, except where such interests are overridden by the fundamental rights of the individual.[23]

21 The application of the legitimate interest ground essentially involves the balancing of the legitimate interests of the organisation (or third party) with the interests or fundamental rights of the data subject,[24] by looking at factors such as public interests, a data subject's reasonable expectations, or the impact on the data subject. An example of legitimate interest is the processing for direct marketing purposes or for preventing fraud, as illustrated in the recitals of the GDPR.[25] Because of the open-ended nature

22 Directive 95/46/EC.

23 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data Art 7(f).

24 Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> (accessed 15 May 2017) (hereinafter "WP29 Report") at p 3.

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (hereinafter "GDPR") Recital 47.

of such a provision, it has been argued that it lacks predictability and legal certainty.[26]

22 In spite of the lack of a bright-line rule, the legitimate interest exception has its attraction in being flexible, while allowing for a principled approach in balancing the interests of the individuals as well as the organisations. It acts as a "catch-all" provision which would cover the "different" or "new" uses of personal data that may not be covered by the other exceptions in the Act, as described above. So, for instance, in the above example, if a company needs to disclose personal data of an individual to clarify the individual's fraudulent misrepresentation of his association with the company, it may be able to do so under the legitimate interest exception since the organisation's reputation and interests are at stake.

23 Permitting the collection, use or disclosure on the basis of "legitimate interests" would provide organisations with an appropriate basis to collect, use and disclose personal data without consent in situations where the rights of the individuals are not compromised. That said, the scope of a possible legitimate interest exception is, admittedly, not without issues and will require further study.

II. Mandatory data breach notification

24 A mandatory data breach notification regime is essentially a legal requirement for organisations to notify certain parties when a data breach has occurred. This typically refers to a situation where personal data have been obtained by, disclosed to or made available to a party without the appropriate authorisation. Under a mandatory data breach notification regime, there may be a requirement to notify the relevant authority, for example, the PDPC, as well as the affected individuals.

25 Under the PDPA, there is no requirement for data breaches to be notified to the PDPC or individuals; although, the PDPC has published a *Guide to Managing Data Breaches*[27] encouraging it as a matter of good practice. Indeed, it may be worthwhile adopting such a practice, given that

26 WP29 Report at p 5.

27 8 May 2015.

early notification of a breach may be a mitigating factor that the PDPC will consider in calculating a financial penalty.[28]

A. Benefits and costs

26 One of the *raison d'êtres* for mandatory data breach notification is to allow individuals whose personal information has been compromised in a data breach to take remedial steps to avoid potential adverse consequences, such as financial loss or identity theft.[29] The benefit to the individual is thus to avoid further harm being caused.[30] It has also been said that a data breach notification empowers individuals with the "right to know" that their information has been compromised.[31]

27 A mandatory data breach notification may also benefit organisations. For example, with a move towards greater accountability on the part of organisations to protect personal data in their possession or under their control, consumers may have greater trust and confidence in the industry knowing that their personal data is being protected, and that in the event a data breach does occur, they will be notified. Organisations may stand to benefit from their customers placing greater trust and confidence in their processes and arrangements to protect personal data.

28 A mandatory data breach notification regime may also benefit society at large. It has been said that a breach notification aids law enforcement, researchers and policy makers in the understanding of the privacy and security environment so that they can develop the necessary policies in this

---

28 Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (21 April 2016) at para 25.3.5.

29 See Australian Government, Attorney-General's Department, *Discussion Paper: Mandatory Data Breach Notification* <https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Consultation-draft-data-breach-notification-2015-discussion-paper.pdf> (accessed 15 May 2017) at p 2.

30 New Zealand Law Commission Report, *Review of the Privacy Act 1993 – Review of the Law of Privacy Stage 4* <https://www.parliament.nz/resource/0000166729> (accessed 15 May 2017) (hereinafter "NZ Law Commission Report") at para 7.16.

31 NZ Law Commission Report at para 7.16.

area. It also alerts the community to the prevalence of data breach incidents.[32]

29 While there are benefits to a mandatory data breach notification regime, it also carries greater compliance costs. Indeed, the main argument against a mandatory data breach notification is that it may come as a "regulatory burden" to the organisation[33] and having to put in place the necessary systems and processes to notify the parties would add to the organisation's costs. This may be especially concerning for small enterprises which may not have the means to afford such a system.

30 These compliance costs are likely to be outweighed by the benefits to organisations. There is some indication that upfront disclosure of a data breach can place an organisation in a more favourable light than one which attempts to cover up a data breach.[34] If an organisation did not notify affected customers of a data breach and the breach became publicly known, the reputational impact and consequent loss of customers could result in a far higher "cost" to the organisation.

B. Key features of regimes in other jurisdictions

31 In this section, the main features of selected data breach notification regimes in Europe (specifically, Regulation 611/2013[35] and the GDPR), the US (specifically, the Civil Code of the State of California) and Canada (specifically, the Alberta's Personal Information Protection Act[36] ("PIPA")) will be considered.

(1) When a data breach notification is required

32 One important element of a data breach notification regime is the criteria which determine when a notification is required. This would

32 NZ Law Commission Report at para 7.16.

33 NZ Law Commission Report at para 7.18.

34 NZ Law Commission Report at para 7.19.

35 Commission Regulation (EU) No 611/2013 of 24 June 2013 on the Measures Applicable to the Notification of Personal Data Breaches under Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications (hereinafter "Regulation 611/2013").

36 SA 2003, c P-6.5.

depend in large part on the underlying objectives of requiring that a notification be provided. For example, if an objective is to prevent harm to the affected individuals, then the notification may be triggered upon discovery that a data breach carries a risk of harm to the affected individuals based on the personal data which had been breached.

33 Under the GDPR, there appear to be differing standards for when a notification to the affected individuals and the supervisory authority are triggered. In relation to notification to the supervisory authority, the controller or processor is required to notify upon becoming aware of a personal data breach unless the breach is unlikely to result in a "risk" to the rights and freedoms of individuals.[37] In relation to the notification to the individuals, the controller is required to notify them of the personal data breach where the breach is likely to result in a "high risk" to their rights and freedoms.[38]

34 The PIPA has a similar threshold which requires notification to be made to the Information and Privacy Commissioner of Alberta where there exists a "real risk of significant harm to an individual".[39]

(2) Parties to notify

35 As noted above, there are mandatory requirements to notify the relevant data protection authority under the GDPR and the PIPA and there is also a mandatory requirement to notify individuals under the GDPR.

36 The PIPA takes a different approach in relation to notification to individuals.[40] Instead of a mandatory requirement to notify individuals, the Alberta Commissioner may, upon being notified of a data breach by an organisation, require the organisation to notify affected individuals. That

37 GDPR Art 33.

38 GDPR Art 34.

39 Personal Information Protection Act (SA 2003, c P-6.5) (Alberta, Canada) s 34.1(1).

40 Personal Information Protection Act (SA 2003, c P-6.5) (Alberta, Canada) s 37.1(1).

said, under the PIPA, organisations may nevertheless voluntarily notify the affected individuals on their own initiative.[41]

(3) Time for notification

37 Generally, the different laws surveyed require the organisation to provide the required notification in an expedient manner. This may be coupled with a maximum time frame for all the notifications to be made (*eg*, within 72 hours), failing which the organisation would have to provide reasons to the data protection authority for its lateness. The GDPR has adopted this approach.[42]

38 Regulation 611/2013 also incorporates an interesting mechanism for a two-tiered notification of the data breach.[43] For the first 24 hours upon detection of the breach, the organisation is permitted to make an initial notification to the relevant data protection authority with certain required information. The organisation may then provide the rest of the required information as soon as possible thereafter, and at most within three days. If the organisation is still unable to provide all the required information, the organisation must submit a reasoned justification within the three-day period and provide the rest of the information as soon as possible.

39 The GDPR allows for the information to be "provided in phases without undue further delay" where the information cannot be provided at the same time.[44]

(4) Contents of notification

40 Across the different laws, there are differing requirements on what is to be notified. Generally, though, the basic information that is to be provided to the affected individuals would include:

---

41 Personal Information Protection Act (SA 2003, c P-6.5) (Alberta, Canada) s 37.1(7).

42 GDPR Art 33(1).

43 Regulation 611/2013 Art 2.

44 GDPR Art 33(4).

(a) information that is sufficient for the data subject to understand the data breach incident and the extent to which it may affect the individual;[45]

(b) information that is sufficient for the data subject to take the necessary steps to avoid or reduce damage incurred;[46] and

(c) contact information of the organisation and the person-in-charge.[47]

41 When it comes to the content of the notification to the data protection authority, there are again differences across the different laws as the notification content needs to be tailored to provide the information required by the data protection authority reacting to the data breach, and this may differ from authority to authority.

(5) Additional obligations of data intermediaries

42 In a case where a data breach involves a data intermediary, the question arises as to whether there should be any obligations imposed on the data intermediary to notify the data protection authority or the affected individuals.

43 In this regard, the GDPR requires data processors (which are similar to data intermediaries under the PDPA) to inform the organisation on whose behalf they are acting (data controller) after becoming aware of a data breach relating to personal data they are processing on behalf of the data controller.[48] However, there is no requirement for the data processor to further inform the relevant data protection authority or the affected individuals.

---

45 See s 1798.29(d)(2) of the Civil Code of the State of California; Art 34(2) of the GDPR and Art 3(4) of Regulation 611/2013.

46 See s 1798.29(d)(3)(B) of the Civil Code of the State of California; Annex II No 9 of Regulation 611/2013 and Art 34(2) referring to Art 33(3) of the GDPR.

47 See s 1798.29(d)(2)(A) of the Civil Code of the State of California; Art 34(2) referring to Art 33(3)(b) of the GDPR and Annex II No 2 of Regulation 611/2013.

48 GDPR Art 33(2).

III. Pseudonymisation

44 Pseudonymisation is a technique to "disguise" personal data, for example, by swapping certain parts of an individual's name with other information which cannot be linked back to the individual so that the name becomes unrecognisable and the individual cannot be identified. Under the GDPR, pseudonymisation is achieved by the separation of information of the personal data such that it can no longer be attributed to a specific data subject without the use of the additional information.[49]

45 Pseudonymisation may allow an organisation to process a set of data for a purpose beyond the purposes for which it was initially collected (a new purpose), where all the personal data in the data set have been psuedonymised (or de-identified in some other fashion). Under Art 6 of the GDPR, where an organisation wishes to use personal data for a new purpose, the use of pseudonymisation will be a factor that goes towards determining whether the new purpose is "compatible" with the original purpose. If it is "compatible" with the original purpose, such use will be permitted under the GDPR.

46 Pseudonymisation is also recognised under the GDPR as forming part of the "appropriate technical and organisational measures" which organisations are required to implement to comply with their obligations under Art 25 of the GDPR (obligation to implement data protection by design and by default) and Art 32 of the GDPR (obligation to ensure security of the personal data).

47 Similarly, pseudonymisation is recognised as a measure that can be used as, or form part of, the safeguards needed for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[50] This is in keeping with the principle of data minimisation under the GDPR.[51]

48 It has been argued that pseudonymised data is not the same as anonymised data, as there is a higher chance of re-identification if an

---

49 GDPR Art 4(5).

50 GDPR Art 89(1).

51 The principle which requires that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed: Art 5(1)(c) of the GDPR.

organisation can obtain the information that was removed from the data set when it was being psuedonymised.[52] Therefore, there remains a risk to the personal data – *ie*, the risk of re-identification – with the use of pseudonymisation. However, with adequate safeguards, the risk of re-identification may just be perceived rather than real.

49 On the other hand, the numerous uses and benefits of pseudonymisation are undeniable. From medical research to market analytics to simply knowing your customers better,[53] pseudonymised data have been, and can be, used for a myriad of purposes. All this, while striking a good balance between, on one hand, allowing organisations to freely use data for their innovative purposes, and on the other, protecting the privacy of individuals.

50 While the PDPA does not have any express provisions on pseudonymisation like the GDPR, it is recognised in the PDPC's anonymisation guidelines[54] as a means of de-identification of personal data.

51 Under the anonymisation guidelines, pseudonymisation is seen as a form of anonymisation technique, which after being applied to the data set, allows the organisation to use the pseudonymised (or anonymised) data set for a variety of uses and purposes, such as transferring the pseudonymised data from one organisation to another.[55] This makes it possible, for example, for organisations to share pseudonymised data for market research with each other. And what makes pseudonymisation particularly useful, more than perhaps the other anonymisation techniques identified in the

---

52 See, *eg*, Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques* <www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf> (accessed 15 May 2017) at pp 10 and 21.

53 As alluded to in Zack Bana (Co-Founder and Data Protection Officer), "Anonymisation: Managing Personal Data Protection Risk" (Personal Data Protection Commission, DPO Connect, November 2015) <http://pdpc.gov.sg/resources/DPO-Connect/november-15/pdf/Anonymisation.pdf> (accessed 15 May 2017).

54 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017).

55 Example given in Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) at para 3.47.

anonymisation guidelines, is where organisations need to ensure that they are dealing with the same data subjects but do not require, or ought not to have, the data subjects' real identities (as pointed out in the *Handbook on European Data Protection Law*).[56] In other words, it is still possible to single out information of the individual for analysis and research, as long as the individual cannot be identified.

52 The anonymisation guidelines also allow for pseudonymised data to be used within an organisation (*ie*, by a department of the organisation) without needing to comply with the data protection provisions of the PDPA since anonymised data are not personal data, but provided that there is "no serious possibility that the data can be used to identify any individual".[57] This means, for example,[58] that a company's marketing department can use pseudonymised data for business analytic purposes, even though the data were originally collected as personal data by the company's customer relations department for the purpose of customer relations. Pseudonymisation could also be a form of protection measure against inadvertent disclosures and security breaches.[59]

53 Overall, based on the GDPR and the latest anonymisation guidelines under the PDPA, there appears to be a trend towards a more permissive approach to the use of pseudonymisation. Given the myriad uses of pseudonymised data, it may be worthwhile for an organisation to consider incorporating such a technique in its system design and process, as a means to protect personal data and to comply with data protection requirements.

---

56 European Union Agency for Fundamental Rights (FRA), Council of Europe and Registry of the European Court of Human Rights, *Handbook on European Data Protection Law* (Luxembourg, 2014) at p 46.

57 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) at para 3.38.

58 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) at para 3.40.

59 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Anonymisation* (revised on 28 March 2017) at para 3.5.

IV. Conclusion

54 As technology continues to advance, data protection laws, too, will need to constantly evolve alongside new technology to ensure that the right balance is struck between the interests of its stakeholders. In keeping pace with these developments, there is a need to look outwardly at global developments which provide useful information of the directions and positions taking place overseas. Through this outward-looking approach, lessons can be learnt and insights can be gained that may aid in shaping this area of law and practice.

MCI (P) 092/07/2017