PERSONAL DATA PROTECTION DIGEST

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

PERSONAL DATA PROTECTION DIGEST

Editor

Yeong Zee Kin

Deputy Editors

David N Alfred

Justin Blaze George

Adeline Chung

Editorial Assistant

Lau Zhong Ning

pdpc

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

2019

CITATION
This volume may be cited as:
[2019] PDP Digest

Published by Academy Publishing

Academy Publishing is a division of the Singapore Academy of Law ("SAL").

SAL 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.

Publicity & Engagement
Personal Data Protection Commission
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438
E-mail: info@pdpc.gov.sg
www.pdpc.gov.sg

MCI(P) 006/07/2019

FOREWORD

BY THE PERSONAL DATA PROTECTION COMMISSIONER

Technological improvements in many domains have led to a transformation in our way of life. Such transformation caused by technology is commonly referred to as "digitalisation".

The benefits of digitalisation are easily observable. Consumers enjoy the convenience of online shopping and can instantly access food delivery and transportation apps on their mobile phones to meet their needs. Businesses have also been quick to harness such benefits, with many establishing online e-commerce channels and tying up with the relevant payment service providers to make the whole digital experience as seamless as possible for the consumer. Some businesses have even forayed into data analytics to predict consumer trends and discover unmet needs.

Amidst all this excitement, it is timely to remember that the success of digitalisation, and its most prominent manifestation – e-commerce – is closely tied to trust, be it consumer trust (in the business-to-consumer context), trust between businesses (in the business-to-business context), or investor confidence in a business. Related to this is the increasing shift from a culture of box-ticking compliance to one that fosters accountability on the part of organisations handling personal data.

The past year has seen various significant global developments aimed at improving the protection of personal data, safeguarding trust and promoting accountability. These are briefly touched on below.

General Data Protection Regulation

The General Data Protection Regulation ("GDPR") came into force on 25 May 2018. The GDPR is groundbreaking in introducing, amongst others, the right to be forgotten, data portability and the concept of "privacy by design". Under the GDPR, an adequacy decision adopted by the European Commission is one of the ways which allow personal data to be transferred outside the European Economic Area. On 23 January 2019, the European Commission and the Personal Information Protection Commission of Japan jointly announced the adoption of decisions recognising each other's personal data protection systems as equivalent. This is the first time the European Union ("EU") and a non-EU country have agreed on

mutual adequacy recognition. South Korea's discussions with the European Commission for an adequacy decision started back in 2015 and are still ongoing.

In the wake of the GDPR, several US states are proposing their own data protection laws that provide certain GDPR-like consumer rights. The California Consumer Privacy Act was signed into law on 28 June 2018 and is set to come into effect on 1 January 2020. The proposed Washington Privacy Act was introduced in the Washington State Senate on 18 January 2019 to update its extant state privacy legislation, and if enacted, would make Washington the second state in the US to adopt a GDPR-styled data privacy law. While the Bill did not advance through the Washington House of Representatives (because of concerns that consumer protections did not go far enough) at the latest legislative session in April 2019, lawmakers have said they will continue to work on this issue during the legislative interim. Whether these initiatives will have the intended effect of leading to a federal data privacy law remains to be seen.

ASEAN

The ASEAN Digital Data Governance Framework was endorsed by ministers of the respective ASEAN member states in December 2018. An objective of this framework is to guide ASEAN member states in their policy and regulatory approaches towards digital data governance and facilitate the harmonisation of data regulations across ASEAN. This follows the adoption of the Framework on Personal Data Protection by the telecommunications and IT ministers of the ASEAN member states in November 2016. Singapore has been active in these initiatives and will continue to do so, in order to ensure that data flows with our more proximate trading partners remain smooth while working collaboratively to build up consumer trust.

Singapore

In February 2018, Singapore became the sixth APEC economy to participate in the APEC Cross-border Data Privacy Rules (alongside the US, Mexico, Canada, Japan and South Korea), and the second APEC economy to participate in the Privacy Recognition for Processors systems (alongside the US). These supranational certification systems enable certified organisations across different jurisdictions to exchange personal data seamlessly, assuring consumers

that the cross-border transfer of their personal data will be subjected to high standards of data protection, as mandated by these systems.

The Data Protection Trust Mark ("DPTM") certification scheme saw its pilot phase in July 2018 and the official launch take place earlier this year. A certified organisation is able to rely on the DPTM to assure its business partners and customers that it adopts transparent and accountable data protection practices. As at 29 April 2019, nine organisations have obtained DPTM certification.

Artificial intelligence ("AI") is a growing part of today's digital economy. In January 2019, Singapore released its Model AI Governance Framework for public consultation, pilot adoption and feedback. This Model Framework is the first in Asia to provide implementable guidance to organisations with respect to addressing key ethical and governance issues when deploying AI solutions.

As part of the ongoing review of the Personal Data Protection Act 2012, Singapore is considering introducing a data portability requirement that would confer greater control and rights by data subjects over the movement of their personal data across service providers. In connection with this, on 25 February 2019, the Personal Data Protection Commission in collaboration with the Competition and Consumer Commission of Singapore released a discussion paper on data portability.

Given the developments above, it therefore comes as no surprise that this third volume of the *Personal Data Protection Digest* includes many articles focusing on these developments and their concomitant issues. As data protection laws evolve to keep pace with technological advances, I believe that this digest will be informative and thought-provoking for organisations and individuals participating in the globally connected digital economy.

I am grateful to our authors who have kindly contributed their invaluable time to share their perspectives on contemporary issues in today's increasingly complex data protection landscape. It is heartening that many of these authors have also penned insightful articles in past volumes of this digest. The Commission encourages practitioners in this field to share their different views in the developing area of data protection law and provides this annual digest as a platform for debate.

Last but not least, I would also like to thank the Law Society of Singapore's Data Protection Sub-committee and Academy Publishing in helping to put together this third volume of the digest.

Tan Kiat How

Commissioner

Singapore

CONTENTS

PERSONAL DATA PROTECTION COMMISSION'S ENFORCEMENT DECISIONS IN 2018: AN OVERVIEW*

Jansen AW†
LLB (National University of Singapore);
CIPP/E, CIPP/A, CIPM, FIP

Natalie Joy HUANG‡
LLB (National University of Singapore)

I. Introduction

1 2018 was a rather momentous year for data protection law, with an unprecedented number of high-profile data breach cases headlining the news both globally and in Singapore.

2 In the months leading up to May 2018, businesses – large multi-national corporations and small to medium enterprises ("SMEs") alike – had urgently sought to adjust their data protection policies to meet the stringent measures under the European Union's General Data Protection Regulations ("GDPR").

3 In March 2018, news broke that British political consulting firm Cambridge Analytica had illicitly harvested the personal data of millions of Facebook users without their consent for political purposes. Given the global extent of the Facebook community, investigations were made as to

---

* Any views expressed in this article are the authors' personal views and should not be taken to represent the views of their employer/law firm. All errors remain the authors' own.

† Of Counsel at LVM Law Chambers LLC.

‡ Intellectual Property lawyer. Natalie represents local and international clients in contentious and non-contentious matters, including copyright and trademark litigation, domain name disputes, TMT and trade secrets litigation, brand enforcement, brand management and commercial transactions. She also advises clients on regulatory issues relating to the music rights clearance, healthcare and data protection.

whether Singapore users' personal data were also affected.[1] Other high-profile cases that made headline news in 2018 include the data breach cases involving Equifax, Marriot, British Airways, and Quora.[2]

4 Closer to home, in June 2018, a major cyberattack on Singapore Health Services Pte Ltd's ("SingHealth") database caused Singapore to experience its most serious data breach to date. Over 1.5 million SingHealth patients' records were accessed and copied, while 160,000 of those had records of their outpatient dispensed medicines records taken as well. Among those affected was Prime Minister Lee Hsien Loong.[3]

5 In January 2019, the Singapore Ministry of Health announced that the HIV-positive status of 14,200 people, along with confidential information such as their identification numbers and contact details, had been leaked online.[4] It was reported that the leak was carried out by an individual who had gained access to the records of the HIV registry in Singapore through his romantic partner.

6 The level and scale of the enforcement activity by the Personal Data Protection Commission ("PDPC") also rose in 2018.

7 In January 2019, the PDPC fined the Integrated Health Information Systems ("IHiS") and SingHealth $750,000 and $250,000, respectively,[5] for breaching their Protection Obligation under s 24 of the Personal Data Protection Act 2012[6] ("PDPA") to protect personal data in their possession or under their control. The fines, amounting to $1m in total, were the highest and second-highest financial penalties imposed by the PDPC to

1 Seow Bei Yi, "Facebook probing if data breach affected Singapore users" *The Straits Times* (23 March 2018).

2 Tom Davies, "A look back at 2018, a landmark year in data protection" *GDPR:Report* (25 December 2018).

3 Kevin Kwang, "Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted" *Channel NewsAsia* (20 July 2018).

4 "HIV-positive status of 14,200 people leaked online" *Channel NewsAsia* (28 January 2019).

5 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376.

6 Act 26 of 2012.

date. Prior to this, the largest financial penalty imposed by the PDPC was $50,000.[7]

8 Apart from increasing in scale, the number of PDPC's enforcement decisions also rose: the PDPC issued 28 decisions in 2018, up from 19 in 2017 and 22 in 2016.

9 Last year also saw the PDPC issue grounds of decision for several less commonly cited obligations under the PDPA such as the Access Obligation, the Accuracy Obligation and the Purpose Limitation Obligation.[8] Overall, however, as in past years, the bulk of the PDPC's enforcement activity in 2018 concerned breaches of the Protection Obligation.[9]

10 Interestingly, even where the organisation under investigation was found to have breached the Protection Obligation, the *manner* in which the Protection Obligation was flouted also evolved. In the past, many organisations were penalised for failing to even put in place *any* data protection policy to take reasonable security steps or arrangements to, *inter alia*, protect the personal data in their possession or under their control. In a number of reported decisions in 2018, however, it was found that simply putting policies in place was not enough; such policies must be adequate to protect personal data.[10]

11 The evolving nature of the breaches of the Protection Obligation is consistent with the general trend of increasing public awareness regarding data protection law. As public awareness increases, it is natural for individuals to seek greater protection over their personal data and for the public to call for more robust protection of personal data.

12 Of note is the PDPC's decision in *Re My Digital Lock Pte Ltd*[11] ("*Re My Digital Lock*"), which dealt, *inter alia*, with how the PDPA sits

---

7 *Re K Box Entertainment Group Pte Ltd* [2017] PDP Digest 1.

8 As defined below.

9 Steve Tan & Michael Chen, "Personal Data Protection Commission's Enforcement Decisions in 2017: Some Lessons to be Learnt" [2018] PDP Digest 1 at para 29.

10 *Re Funding Societies Pte Ltd* [2019] PDP Digest 341; *Re Institute of Singapore Chartered Accountants* [2019] PDP Digest 333.

11 [2018] PDP Digest 334.

within the framework of statutory and common law rights that collectively provide safeguards to individuals in Singapore.

13 By focusing on the PDPC's enforcement activity in 2018, this article will proceed to discuss (non-exhaustively) the general trends in the data protection sphere and the lessons that can be gleaned from the PDPC's reported decisions.

II. Evolving nature of breaches of the Protection Obligation

14 In 2018, as was the case in 2016 and 2017,[12] breaches of the Protection Obligation remained the most common among the PDPC's reported decisions. Among the PDPC's 28 reported decisions in 2018, 19 concerned breaches of the Protection Obligation.

15 Notably, the nature of such breaches of the Protection Obligation has somewhat evolved.

16 In the first survey of the PDPC's enforcement activity in 2016, it was remarked that in a number of the enforcement decisions, many organisations appeared to lack an overall awareness of and sensitivity to the data protection obligations under the PDPA, in particular the Protection Obligation.[13]

17 In 2018, there were still some organisations similarly taken to task for failing to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. For example, in *Re Bud Cosmetics*,[14] in the absence of any security arrangements to protect the personal data in question from unauthorised disclosure, the organisation in question was fined $11,000 for contravening the Protection Obligation.[15] Directions were also issued to the organisation to engage

12 Steve Tan & Michael Chen, "Personal Data Protection Commission's Enforcement Decisions in 2017: Some Lessons to be Learnt" [2018] PDP Digest 1 at para 29.

13 Lim Chong Kin & Charmian Aw, "A Survey on Enforcement of the Personal Data Protection Act 2012" [2017] PDP Digest 255 at para 10.

14 [2019] PDP Digest 351.

15 *Re Bud Cosmetics* [2019] PDP Digest 351 at [27].

qualified personnel to conduct a security audit, develop an IT security policy, and implement a training policy.[16]

18 However, it is not enough for companies to simply ensure that they have some policies and processes on data protection in place. The risk and threats to data security are constantly evolving and increasing in sophistication, and there is a need to match these with the same sophistication of protection.

19 For example, the cyberattack on SingHealth's patient database system serves as a good example of how an organisation, despite having in place a number of security arrangements to protect the personal data in its possession or under its control, found itself in the midst of the worst data breach in Singapore.

20 SingHealth, a Singapore public healthcare institution ("PHI"), belongs to one of three healthcare clusters in the Singapore public healthcare sector ("Clusters"). Its primary function is the provision of healthcare services. Within each Cluster, a group chief information officer ("GCIO") is charged with (among other things) security oversight for that Cluster and assisting the Cluster with its IT security program.

21 IHiS, the central national IT agency for the public healthcare sector in Singapore, was established in July 2008 to centralise all of the IT functions and capabilities of Singapore's PHIs (including IT staff) in a single entity, which would support all the PHIs. IHiS also assumed responsibility for the development and maintenance of the Clusters' IT systems (including SingHealth's).[17]

22 At the time of the data breach, IHiS had management over the day-to-day operations and technical support, maintenance and monitoring of the entire SingHealth IT system, including SingHealth's Sunrise Clinical Manager system ("SCM") and the other Clusters' IT systems.[18]

23 Between 27 June and 4 July 2018, the personal data[19] of 1,495,364 unique individuals were illegally accessed and copied from the SCM

16 *Re Bud Cosmetics* [2019] PDP Digest 351 at [37].

17 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [8].

18 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [12].

19 This included the names, NRIC numbers, addresses, gender, race, and dates of birth of 1,495,364 SingHealth patients, and the outpatient dispensed

(*continued on next page*)

database. Outpatient prescription records of nearly 160,000 patients were also exfiltrated.[20]

24 The issues before the PDPC were whether (a) IHiS was acting as a data intermediary for SingHealth in relation to the SingHealth patients' personal data on the SCM database; and (b) SingHealth and/or IHiS complied with the Protection Obligation in respect of the data breach.

25 The PDPC ultimately found that IHiS, as a data intermediary of SingHealth, had an obligation to make reasonable security arrangements to protect the personal data of SingHealth's patients in its possession or under its control.[21] As for SingHealth, it had the primary responsibility of ensuring that there were reasonable security arrangements in place to protect the personal data in its possession or under its control, regardless of whether it had appointed a data intermediary to process patient personal data on its behalf.[22]

26 The *Re Singapore Health Services Pte Ltd* ("*Re SingHealth*") decision serves as a reminder that while organisations may outsource work to vendors, the responsibility for complying with statutory obligations under the PDPA may not be delegated.

27 In its grounds of decision, the PDPC highlighted in some detail the various security arrangements SingHealth had in place to meet its supervisory role for the protection of personal data.[23] These security arrangements included a data protection policy, a PDPA employee standards manual, a dedicated Intranet page for PDPA training materials accessible to all staff, a master data share agreement to regulate the sharing of information among SingHealth institutions, a data access approval policy and a data breach management policy.

28 Yet, notwithstanding these data protection measures, the PDPC found a critical failure in SingHealth's IT security incident reporting

---

medication records of 159,000 patients (which is a subset of the full set of illegally accessed personal data).

20 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [1].

21 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [44].

22 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [54].

23 See *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [65] and [66].

process.[24] Although the SingHealth cluster information security officer was informed of suspicious activities showing multiple failed attempts to log in to the SCM database using invalid credentials, accounts that had insufficient privileges in mid-June 2018, and the attack and remediation efforts on 4 July 2018, he did not escalate these security events. Ultimately, his failure to do so led to a finding that he had failed to discharge his duties – a lapse attributable to SingHealth.[25]

29 Similarly, IHiS, which maintained a comprehensive IT security incident and response framework,[26] was also found in breach of the Protection Obligation under the PDPA.[27] Amongst other things, the PDPC had found some fundamental weaknesses in the security of the system, such as (a) inadequate implementation of IHiS's policies and practices, (b) weak local administrator passwords, (c) failure to disable dormant accounts, (d) lack of controls to detect bulk querying behaviours, (e) failure to patch software, (f) failure to remediate previously detected vulnerabilities, and (g) failure of staff to recognise suspicious activity and to escalate it.[28]

30 The *Re SingHealth* decision is a timely reminder of the insufficiency of merely having in place or disseminating data protection policies and instructions to staff members. In another 2018 decision, *Re SLF Green Maid Agency*,[29] the PDPC noted that where an organisation handles large volumes of sensitive personal data, it must ensure that its employees are aware of such guidelines through structured and periodic training. In the *Re SingHealth* decision, the PDPC once again reiterated that regular training sessions and staff exercises should have been conducted to ensure that all IHiS staff were familiar with the IT security incident reporting and their role in recognising and reporting suspected IT security incidents.[30]

31 In other cases involving breaches of the Protection Obligation, the less severe nature and extent of the data breaches in question was reflected in the penalties imposed by the PDPC. For example, in *Re Funding Societies Pte*

24 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [58].
25 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [84].
26 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [102]–[104].
27 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [134].
28 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [110]–[127].
29 [2019] PDP Digest 327 at [13].
30 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [107].

Ltd,[31] a financial penalty of $30,000 was imposed on the organisation for failing to make reasonable security arrangements to prevent the unauthorised disclosure of the personal data of 4,000 of its members. In *Re WTS Automotive Services Pte Ltd*,[32] a financial penalty of $20,000 was imposed on the organisation for breaching the Protection Obligation. The data breach incident concerned the personal data of some 2,471 of the organisation's customers.

32 The many cases dealing with breaches of the Protection Obligation in 2018 reveal that protective measures still remain the Achilles heel for many organisations. Some have suggested that the standard underpinning the Protection Obligation (and indeed all obligations under the PDPA), namely "what a reasonable person would consider appropriate in the circumstances",[33] ought to take into account the resource-scarce reality of small organisations when determining if they have discharged their obligations under the PDPA.[34]

33 Nevertheless, the penalties that the PDPC has meted out have been balanced and proportionate. For example, to reflect the severity and extent of the SingHealth data breach, the financial penalties imposed on SingHealth and IHiS were by far the largest two penalties imposed on organisations for breaching the PDPA (for context, K-Box comes in at a modest third with $50,000). The quantum of these penalties, the PDPC said, was appropriate given that it was the largest data breach suffered by any organisation in Singapore and involved highly sensitive and confidential personal data.[35] In other cases, the PDPC has issued relatively modest financial penalties of between $500 and $25,000 or a warning, presumably to take into account the relatively less severe nature of these data breaches and the fact that the organisations involved were SMEs.[36]

---

31 [2019] PDP Digest 341.

32 [2019] PDP Digest 317.

33 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(1).

34 Foo Ee Yeong Daniel, "Suggestions on the relevance of the Organization's Size to Section 11 of Singapore's Personal Data Protection Act" (2018) 9 *Juris Illuminae* (17 January 2018).

35 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [138]–[139].

36 Lim Chong Kin & Charmian Aw, "A Survey on Enforcement of the Personal Data Protection Act 2012" [2017] PDP Digest 255 at para 20.

III. Accuracy, Access and Purpose Limitation Obligations

34 Aside from an increasing trend toward more sophisticated breaches, 2018 also saw the PDPC issue grounds of decision in respect of several more uncommonly cited obligations under the PDPA.

A. Accuracy Obligation

35 In May 2018, the PDPC issued its first grounds of decision in *Re Credit Bureau (Singapore) Pte Ltd*[37] ("*Re Credit Bureau*") regarding an organisation's obligation under s 23(*b*) of the PDPA to make a reasonable effort to ensure that the personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be disclosed by the organisation to another organisation ("Accuracy Obligation").

36 The *Re Credit Bureau* decision stemmed from a complaint by an individual who had a bankruptcy application taken out against him in June 2012 and withdrawn a month later. The complainant was given a "HX" risk grade in his Enhanced Consumer Credit Report, which meant there could be a past or existing bankruptcy record associated with him. The complainant felt that a "HX" risk grading was inaccurate as he thought this implied he had an outstanding bankruptcy record or was not creditworthy. When he requested that the organisation amend his risk grading, he was told it was the organisation's practice to display bankruptcy-related data for five years. The complainant lodged a complaint with the PDPC that the organisation had retained his personal data when it was no longer necessary for legal or business purposes.[38]

37 The organisation explained that the "HX" rating merely meant there was a past or existing bankruptcy record associated with that particular individuals; the "HX" rating alone did not determine creditworthiness. Public registry searches would also reveal that the complainant was not a bankrupt. For these reasons, the PDPC found that the organisation had not breached the Accuracy Obligation under the PDPA.[39]

---

37 [2019] PDP Digest 227.

38 *Re Credit Bureau (Singapore) Pte Ltd* [2019] PDP Digest 227 at [2]–[3].

39 *Re Credit Bureau (Singapore) Pte Ltd* [2019] PDP Digest 227 at [7] and [11].

B. Access Obligation

38 The Access Obligation took the spotlight in *Re Management Corporation Strata Title Plan No 4436*.[40] A subsidiary proprietor requested to view CCTV footage of the condominium grounds to locate a missing cat in the presence of two council members pursuant to s 47 of the Building Maintenance and Strata Management Act[41] ("BMSMA"), which allows any subsidiary proprietor to ask for inspection and request a copy of any record or document in the possession of a management corporation. Two other subsidiary proprietors of the condominium complained to the PDPC, citing concerns that other individuals might be captured in the said CCTV footage.

39 The issue was whether, in allowing that subsidiary proprietor to inspect such CCTV footage, the management corporation was in breach of s 21 of the PDPA, which gives a data subject the right to access personal data about him that the organisation has in its possession or under its control, subject to the restrictions under ss 21(2) and 21(3) ("Access Obligation"). Under s 21(3)(*c*) of the PDPA, an organisation cannot provide access to personal data that can reasonably be expected to reveal personal data about another individual.

40 In the face of the inconsistent provisions in s 47 of the BMSMA and s 21 of the PDPA, the subordination provision in s 4(6)(*c*) of the PDPA became operative to place the PDPA provisions in subordination to other written law, such that the provisions of such other written laws would prevail in the event of any inconsistencies.

41 Thus, the PDPC was obliged to decide that s 47 of the BMSMA prevailed over s 21 of the PDPA, and consequently the management corporation could provide inspection of the CCTV footage to a subsidiary proprietor without the need to redact personal data of other individuals or to seek their consent for such disclosure.[42]

---

40 [2019] PDP Digest 264.

41 Cap 30C, 2008 Rev Ed.

42 *Re Management Corporation Strata Title Plan No 4436* [2019] PDP Digest 264 at [14].

C. *Purpose Limitation Obligation*

42 The PDPC also issued four decisions[43] regarding breaches of the obligation to collect and use personal data only for purposes that a reasonable person would consider appropriate in the circumstances and for which the affected individual has been informed ("Purpose Limitation Obligation").[44] The PDPC has only issued one other grounds of decision regarding the Purpose Limitation Obligation.[45]

43 Of note is *Re Club the Chambers*,[46] which concerned the posting in the organisation's premises of notices comprising enlarged photocopies of identity documents belonging to individuals who had been banned from the premises. The organisation stated that the purpose of the display of notices was to assist its staff in identifying banned members and to inform banned members that they were prohibited entry into the LAN shop.[47] However, the PDPC found that, under s 18 of the PDPA, a reasonable person would not consider it appropriate to display the notices to everyone who enters the LAN shop. Rather, there were other better ways to inform staff and banned members of the ban, such as by maintaining an internal blacklist only available to staff on duty.[48]

44 Ultimately, the manner in which the organisation had disclosed personal data, which effectively was a form of "naming and shaming" of individuals, did not accord with the Purpose Limitation Obligation. The organisation was found in breach of the Purpose Limitation Obligation. The PDPC's decision brings clarity and is a welcome guidance to organisations looking to maintain a blacklist for their businesses.

---

43 *Re Actxa Pte Ltd* [2019] PDP Digest 156; *Re Spring College International Pte Ltd* [2019] PDP Digest 230; *Re Galaxy Credit & Investments Pte Ltd* [2019] PDP Digest 288 and *Re Club the Chambers* [2019] PDP Digest 304.

44 See s 18 of the Personal Data Protection Act 2012 (Act 26 of 2012).

45 *Re AIA Singapore Private Limited* [2017] PDP Digest 73.

46 [2019] PDP Digest 304.

47 *Re Club the Chambers* [2019] PDP Digest 304 at [14].

48 *Re Club the Chambers* [2019] PDP Digest 304 at [19].

IV. Data protection and privacy

45 As technology evolves and data collection becomes part of everyday life, many organisations seeking to tap such technology must also grapple with issues concerning the privacy of individuals.

46 In the seminal 2018 decision of *Re My Digital Lock Pte Ltd*[49] ("*Re My Digital Lock*"), the PDPC clarified for the first time several issues fundamental to the administration and enforcement of the PDPA – namely, the interaction between the applicable common law principles protecting privacy and the operation of the PDPA. The discourse in *Re My Digital Lock* highlights that whilst data protection and privacy laws are often conflated, they are not the same thing in respect of the PDPA.

47 In *Re My Digital Lock*, the organisation in question posted a police report made against the complainant on Facebook. The complainant said the Facebook post disparaged his reputation and amounted to a wrongful disclosure of his personal data under the PDPA.

48 In an illuminating analysis, the PDPC traversed the various privacy laws in Singapore and the distinctions between such laws and the PDPA.[50] While there were overlaps in the PDPA and privacy, especially informational privacy, the PDPC observed that the PDPA was not intended to cover other areas of privacy. In this case, the PDPC found that the nature of complaint was rooted in other areas of privacy, such as false light publicity (*ie*, defamation), and it was not a suitable complaint to be investigated under the PDPA. In the final analysis, the PDPC took the position that the courts were better placed to decide on the legal issues arising from the claim, especially given the incipient nature of privacy laws in Singapore.

49 Looking ahead, it seems unrealistic to study or critique data protection law in isolation. As *Re My Digital Lock* has shown, individuals are becoming increasingly aware of not just the value of their personal data to businesses, but of the value of protecting their privacy in and of itself. In this regard, there may yet be room for privacy laws in Singapore to develop and this may require revisiting the intersection of such laws with the PDPA.

---

49 [2018] PDP Digest 334.

50 *Re My Digital Lock Pte Ltd* [2018] PDP Digest 334 at [25].

V. Conclusion

50 2018 saw various watershed moments in public understanding of what it means to protect personal data in Singapore. Unlike the European human rights-centric approach to data protection, a main aim of the enactment of the PDPA was to strengthen Singapore's overall competitiveness and enhance its status as a trusted hub and choice location for global data management and processing services.[51]

51 For businesses, the ability to harness and make use of personal data provides an edge over competitors. Yet the push to become more competitive by harnessing and collecting individuals' personal data must be balanced with legitimate public concerns regarding exploitation of personal data and the safeguards in place to protect an individual's personal data and privacy.

52 The PDPC's willingness to draw out these issues in *Re My Digital Lock* and its other published decisions is encouraging. As public awareness and interest develops in this space, we can only expect data protection and privacy laws to grow in importance. The continuous strive by companies to improve their data protection processes will be crucial for Singapore to maintain its status as a trusted technology and data processing hub.

---

51 *Parliamentary Debates, Official Report* (15 October 2012), vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communication and the Arts).

EMBRACING ACCOUNTABILITY IN THE CONTEXT OF PERSONAL DATA PROTECTION AS UNDERSTOOD FROM THE PERSONAL DATA PROTECTION COMMISSION'S ENFORCEMENT DECISIONS IN 2018[*]

Steve TAN[†]
LLB (National University of Singapore),
LLM (University College London);
CIPP/A

Michael CHEN[‡]
JD (Melbourne Law School)

---

* Any views expressed in this article are the authors' personal views and should not be taken to represent the views of their employer/law firm. All errors remain the authors' own.

† Partner and Deputy Head in Rajah & Tann Singapore's TMT (Technology, Media and Telecommunications)/Data Privacy practice group. Highly regarded for his expertise in data privacy and technology law work, Steve has pioneered several new data protection related services which organisations have found valuable. Steve has been recognised as a leading lawyer in *PLC Cross-border Media and Communications Handbook*, *Asia Pacific Legal 500*, *AsiaLaw Profiles*, *Practical Law Company Which Lawyer*, *Chambers Asia Pacific*, *Best Lawyers*, *The International Who's Who of Telecoms and Media Lawyers*, and *Who's Who Legal: Data*. Steve has been named Communications Lawyer of the Year in the Corporate Livewire 2015 Legal Awards and in Corporate Insider Business Excellence Award 2019. Steve is cited as "one of the best in the field of personal data protection" in *Legal 500* 2017 and as being "one of the gurus in the field of data protection" in *Legal 500* 2019. Steve is a Certified Information Privacy Professional (Asia) (CIPP/A).

‡ Formerly an Associate in Rajah & Tann Singapore's TMT/Data Privacy practice group. Before embarking on his legal career, he worked as a computer engineer in the information security field, with experience in computer, communications and e-commerce platforms and software.

I. Introduction

1 In response to the evolving digital landscape, significant developments to Singapore's data protection law were proposed or occurred in 2018. As part of the ongoing review of the Personal Data Protection Act 2012[1] ("PDPA"), the Personal Data Protection Commission ("PDPC") issued a public consultation on 27 April 2018 entitled "Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy" ("Consultation Paper"), under which it was proposed that the Do Not Call ("DNC") provisions and the Spam Control Act[2] be merged into a single legislation governing all unsolicited commercial messages. In addition, the PDPC proposed to introduce an Enhanced Practical Guidance ("EPG") framework for the PDPC to provide organisations guidance with regulatory certainty regarding complex or novel compliance issues.

2 The PDPC also sought feedback under the Consultation Paper regarding the exceptions for the collection, use and disclosure of personal data without consent in the Second, Third and Fourth Schedules to the PDPA, as a follow-up to its *Public Consultation for Approaches to Managing Personal Data in the Digital Economy*, previously issued in July 2017 (the "2017 Digital Economy Consultation").

3 On 31 August 2018, the PDPC issued its *Advisory Guidelines On The PDPA For NRIC And Other National Identification Numbers*, to clarify how the PDPA applies to organisations' collection, use and disclosure of NRIC and other national identification numbers, and retention of physical NRIC or other identification cards by organisations, including activities which organisations are prohibited from carrying out in dealing with identification numbers or cards. In addition, the PDPC issued the *Technical Guide to Advisory Guidelines on the PDPA for NRIC and Other National Identification Numbers* to provide useful suggestions that organisations could consider in replacing NRIC numbers for identifying individuals on their websites and other public facing computer systems.

4 The PDPC has provided further guidance regarding other pertinent data protection issues; for instance, the *Guide to Basic Data Anonymisation*

1 Act 26 of 2012.

2 Cap 311A, 2008 Rev Ed.

Techniques (published 25 January 2018), *Guide to Data Sharing* (updated 1 February 2018), *Guide for Printing Processes for Organisations* (published 3 May 2018), and *Guide on Building Websites for SMEs* (revised 10 July 2018).

5 The developments summarised above are a continuation of the PDPC's efforts to pivot from a culture of compliance to accountability in personal data management, whereby organisations are encouraged to adopt a culture of accountability and demonstrate to customers and data subjects that they have proactively identified and addressed risks to personal data. The Data Protection Trustmark certification scheme, which was launched by the Infocomm Media Development Authority and PDPC in January 2019, will be a key element of the pivot to accountability, through which certified organisations can better gain consumers' trust and thereby obtain competitive advantage. The impending mandatory data breach notification regime described in the 2017 Digital Economy Consultation enshrines the accountability of organisations to individuals whose personal data they are processing, through notification of a data breach occurring with respect to those individuals' personal data.

6 With the PDPA having been in force for over four years, organisations must now recognise that the concept of accountability is in fact conceptually and spiritually embedded within the PDPA even though there may be no express wording as such. The mandatory need for each organisation to appoint at least one data protection officer,[3] to have policies and practices to meet the PDPA requirements[4] and to expressly state that each organisation is responsible for personal data within its possession or control[5] are some examples of the hallmark of accountability.

7 In order to strengthen their accountability practices, organisations would do well to extract key areas of guidance from the PDPC's enforcement decisions. The decisions issued in 2018 provide valuable guidance on the practices that should be taken pursuant to the PDPA's data protection provisions, so that organisations may better demonstrate their accountability in personal data protection. This article will also highlight

3 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(3).
4 Personal Data Protection Act 2012 (Act 26 of 2012) s 12.
5 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(2).

additional pertinent lessons that can be gleaned from some of the 2018 enforcement decisions.

II. Overview of the enforcement decisions issued by the Personal Data Protection Commission in 2018

8 The PDPC remains active in enforcing the PDPA, having issued 29 reported decisions[6] in 2018, as compared to 19 reported decisions in 2017. Where breaches of the PDPA were found, the organisations in question were punished with financial penalties and/or directions for compliance, or were given warnings.

9 Similar to 2017, a significant majority of the decisions (19 out of the abovementioned 29) involved a finding by the PDPC that there was a breach of the Protection Obligation under the PDPA. This was followed by the "Consent Obligation", and then the "Purpose Limitation Obligation", "Notification Obligation", and "Openness Obligation".

10 Most of the cases were initiated by complaints to the PDPC. Where there was a complaint, many of the organisations involved were unaware that a breach (or potential breach) of the PDPA had occurred. In some cases, the complainant first made a complaint to the organisation, and only subsequently complained to the PDPC when the organisation did not respond or take remedial action – this shows that a formal complaint by an individual to the PDPC can be avoided if the organisations in question had taken the commercially astute approach of acknowledging and dealing with the complainant in the first place.

11 The specific lessons that can be gleaned from some of the 2018 enforcement decisions will be elaborated on below. Many of the lessons relate to organisations' accountability for protecting personal data in their possession or control.

---

6 It is pertinent to note that the reported decisions are not indicative of the number of investigations or cases undertaken by the Personal Data Protection Commission. Some cases may not be the subject of a reported decision.

III. Embracing accountability, as understood from the 2018 enforcement decisions

12 Under the concept of accountability, organisations are answerable to the individuals whose personal data they possess or control, and to the PDPC; this is described in the PDPC's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017).

13 The PDPC has provided guidance to organisations on how to conduct data protection impact assessments and implement data protection management programmes, through the *Guide to Data Protection Impact Assessments* and *Guide to Developing a Data Protection Management Programme*, respectively (both published 1 November 2017).

14 Further guidance can be gleaned from the enforcement decisions in 2018, which reinforce the importance of various measures that organisations must take to demonstrate their accountability in data protection management. Some of the categories in which these measures can be broadly grouped under are: (a) risk assessment, mitigation and remediation; (b) policies, processes and training; and (c) transparency. These categories will be described in further detail below.

A. Risk assessment, mitigation and remediation

15 As part of the pivot from a culture of compliance to accountability, and in the light of the impending proposed changes to the PDPA, organisations will be expected to proactively identify, assess and mitigate the risks to personal data in their systems and processes.

16 With regard to online systems or websites that organisations deploy for their customers' use, organisations need to implement relevant security arrangements such as the regular conduct of vulnerability assessment or penetration testing for such systems/websites. In *Re WTS Automotive Services Pte Ltd*,[7] the PDPC made clear that penetration test(s) or vulnerability assessment(s) must be carried out prior to a website being made accessible to the public including thereafter on a periodic basis, such as annually. The failure to do so would be a breach of the Protection Obligation.

---

7 [2019] PDP Digest 317.

17 The lack of requisite technical expertise within an organisation's staff to manage its complex IT systems is no excuse. The organisation must in such a case engage competent service providers with the relevant technical expertise to assist the organisation.[8] By doing so, the organisation would then be able to demonstrate that it is taking its obligations and responsibilities under the PDPA seriously. When engaging such a third-party service provider, an organisation is expected to properly document in the contract between the organisation and such service provider the organisation's requirements with respect to the protection of the organisation's personal data, prior to the provision of services by the service provider. Post-execution of the contract, the organisation cannot simply rely on and believe that the third-party service provider will do the right thing. Instead, the organisation has to regularly follow up by ensuring that the service provider is indeed delivering the services properly and protecting the personal data in accordance with the PDPA.[9] In other words, the expectation is that an organisation that has engaged a third-party service provider to process personal data on its behalf has to have oversight of the third-party service provider during the course of the engagement.

18 Another case that illustrates the above theme is *Re Singapore Cricket Association*,[10] which involved the unauthorised disclosure of cricket players' personal data on the Singapore Cricket Association's website. This was a classical case concerning the responsibility that an organisation has when it engages a third-party service provider to develop a website that would contain personal data – the organisation must ensure that the personal data is adequately protected and provide the service provider with clear written instructions dealing with the handling of personal data. Such instructions should be written into the contract. It is certainly not enough for the instructions to be conveyed piecemeal in meetings, and through phone calls and WhatsApp text messages, which would likely lead to confusion over the engaging organisation's exact requirements.

19 Hence, in the case when an organisation is transferring personal data to a third-party service provider to perform the services or when the latter is handling personal data on the former's behalf, the organisation needs to

8 *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [24].

9 *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [16] and [17].

10 [2019] PDP Digest 270 at [27].

carefully assess the risk to the personal data and put in place measures to mitigate such risk. In most cases, this can be done by (a) ensuring that the written contract has robust and suitable clauses dealing with personal data protection; and (b) the organisation continually monitoring the third-party service provider's performance of the services and handling of the personal data.

20 Various factors go into the assessment of risk to personal data and one of the key ones is the level of sensitivity of personal data. As enunciated by the PDPC in *Re Aviva Ltd*,[11] the greater the sensitivity of the personal data in question, the higher the expectation of protection measures to be put in place in handling the personal data.

21 Where an organisation puts in place a new IT system or process, it is imperative that not only user acceptance testing be carried out but also the nature or type of testing in question should be comprehensive and able to cover the foreseeable risks that may occur for personal data arising from the system or process.[12]

22 In this digital economy, many organisations deploy websites or online platforms to conduct business with their customers. It is a given that before such a transactional website goes live, it must have been tested and checked for vulnerabilities with the objective of ensuring that personal data that may be disclosed or accessed by authorised users of the website are adequately protected, pursuant to the PDPA's Protection Obligation. As part of operations, such transactional websites often are modified, improved upon or upgraded with new components or modules. Similar to the case where organisations have reviewed the functionality and security of transactional websites before they go live, in the case where modifications are to be made to existing websites, organisations need to review, test and ensure that the modifications do not create vulnerabilities to the website such that personal data may be compromised. The PDPC decision of *Re Funding Societies Pte Ltd*[13] illustrates the care that organisations must undertake when carrying out modifications to their transactional websites through which personal data may be accessed or disclosed – security testing of the website for vulnerabilities is a must. If vulnerabilities are found in an organisation's

11 [2019] PDP Digest 145 at [17].

12 *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 189 at [30].

13 [2019] PDP Digest 341 at [29].

systems that place personal data at risk, the organisation must remediate and remove the vulnerability immediately. Where such remedial measure requires the website accessibility to be suspended pending completion of remediation, the organisation should do so as personal data is placed at risk if remediation is not done.

23 In the event that there are vulnerabilities in an organisation's website that result in the compromise or unauthorised disclosure of personal data, the fact that the organisation in question is a young organisation is neither an excuse nor a mitigating factor that the PDPC would take into consideration.[14] All organisations are expected to fully comply with the PDPA regardless of the age of the organisation.

24 Organisations are ever more leveraging technology to improve their operations or as an extension of their embracing the digital economy. In doing so, organisations must assess the risks to personal data within their possession or control, posed by the new technology or online platform that they are deploying. Though the decision to leverage technology is laudable in terms of improving operations or the customer experience, organisations must carefully assess the pitfalls, if any, with respect to the protection of personal data, in deploying the technology or new online platform. The decision in *Re Singapore Management University Alumni Association*[15] exemplifies the need for organisations to appropriately assess the sufficiency or otherwise of security measures to protect personal data with respect to the utilisation of a technology or a new website/online platform before such new technology or website/online platform goes live. The use of identification numbers alone to serve the separate functions of identification and authentication to access personal data on a website will not constitute reasonable security arrangements that is required by the Protection Obligation. Another decision, namely *Re Jade E-Services Singapore Pte Ltd*,[16] illustrates the need to fully understand and/or appropriately deploy the technology in question as failure to do so may lead to an unexpected consequence of placing personal data at risk of exposure. This latter case dealt with the deployment of a bot manager service for the organisation's website.

---

14 *Re Funding Societies Pte Ltd* [2019] PDP Digest 341 at [33].

15 [2019] PDP Digest 170 at [22].

16 [2019] PDP Digest 285.

B. Policies, processes and training

25 In dealing with compliance with the PDPA, organisations should carefully consider any additional internal processes that they need to implement in order to remove or reduce the risk of human error. Even though an organisation may have multiple PDPA-related policies, personal data could be compromised due to human error on the part of its employees. Key to avoiding a finding of a breach of the Protection Obligation is whether the organisation has implemented processes that could reasonably seek to deal with the potentiality of such human error. It is no excuse, if a breach of the Protection Obligation occurs, that an organisation trusted that its employee would do the right thing.[17] Depending on the operational activity in question, such processes could entail the carrying out of institutionalised random checks on the work or activity of the employees in question that are handling the personal data.

26 When implementing security arrangements to protect personal data, organisations should take heed of the PDPC's view that it is not advisable for an organisation to rely on a member of its staff checking *his own work* to ensure that he has undertaken a task properly to meet the organisation's protection obligation under s 24 of the PDPA.[18]

27 It cannot be emphasised enough the importance of training of staff on the requirements of the PDPA in enabling an organisation to comply with the PDPA. In fact, training is a key element of complying with the Protection Obligation. Proper comprehensive training can facilitate the staff's subsequent ability to consider PDPA implications when they encounter novel operational issues where personal data is involved. It was found by the PDPC in *Re SLF Green Maid Agency*[19] that the organisation had not provided its staff with formalised training on personal data. In this case, the organisation's staff had re-used paper containing personal data of individual(s) to write information responding to a customer's queries and handed over such paper to the customer.

28 Data protection training can help an organisation comply with the Openness Obligation under the PDPA in that through the training,

17 *Re Aviva Ltd* [2019] PDP Digest 145 at [15].

18 *Re NTUC Income Insurance Co-operative Ltd* [2019] PDP Digest 208 at [17].

19 [2019] PDP Digest 327 at [8], [12] and [13].

the organisation can communicate its PDPA-related policies and practices to its staff.[20]

29 It is by now well understood that every organisation needs to have policies to assist the organisation to comply with the PDPA and that such policies need to be communicated to its staff. As part of an organisation's operational activities, there could be some activities where no personal data is involved and others where personal data is involved. Organisations should assess the need for having specific policies or standard operating procedures to deal with specific operational activities where personal data is involved or being handled.[21]

C. *Transparency*

30 Establishing and operationally deploying a privacy policy is a key accountability practice that enables an organisation to demonstrate transparency in its activities involving personal data. Many organisations rely on their respective privacy policies to notify individuals of the purposes by which personal data may be processed, and to obtain consent, for the collection, use and disclosure of personal data. Apart from the organisation having to bring the privacy policy to the attention of the individual and obtaining his consent to the privacy policy before collecting that individual's personal data, the organisation needs to ensure that the contents of the privacy policy adequately inform the individual of the situations in which that individual's personal data may be collected, in particular when an organisation is utilising Internet of Things ("IoT") devices or an uncommon means to collect personal data as opposed to merely through the website in question.

31 In the case of *Re Actxa Pte Ltd*,[22] Actxa sold healthcare and fitness related IoT devices, such as smart weighing scales and fitness trackers, and provided the Actxa app to customers, while relying on its website privacy policy to notify its customers of the purposes for which Actxa would be processing personal data and to obtain consent for the collection, use and disclosure of their personal data via the various IoT devices and Actxa app.

---

20 *Re Habitat for Humanity Singapore Ltd* [2019] PDP Digest 200 at [14].

21 *Re Habitat for Humanity Singapore Ltd* [2019] PDP Digest 200 at [13].

22 [2019] PDP Digest 156.

However, the website privacy policy did not contain any reference to the collection, use and disclosure of personal data through the Actxa app or IoT devices, and instead only referenced the Actxa website.

32 The PDPC decided that it was not enough to rely on a general website privacy policy that did not expressly address the collection, use, and disclosure of personal data by the organisation's other products and platforms, such as the IoT devices and Actxa app.[23] Accordingly, the PDPC held that there was a breach of the Consent Obligation and Purpose Limitation Obligation under the PDPA.

IV. Conclusion

33 This article has highlighted pertinent lessons relating to accountability practices that can be gleaned from some of the enforcement decisions issued by the PDPC in 2018. As was the case in 2017, many of these lessons pertain to the Protection Obligation. Notwithstanding the aforesaid, many organisations have also been taken to task for breaching other PDPA obligations. By taking heed of these lessons, organisations may better demonstrate their accountability in personal data protection and reap the benefit of gaining their customers' trust.

---

23 *Re Actxa Pte Ltd* [2019] PDP Digest 156 at [22]–[24].

PURPOSE LIMITATION OBLIGATION: THE APPROPRIATE PURPOSE REQUIREMENT*

Benjamin WONG YongQuan†
LLB (National University of Singapore); Advocate and Solicitor (Singapore)

I. Introduction

1 The principle of purpose limitation is a well-established principle in data protection law. It has been justifiably described as "a cornerstone of data protection".[1] In Singapore, it is also an aspect of the legislative purpose of the Personal Data Protection Act 2012[2] ("PDPA"). As its name suggests, the principle of purpose limitation is that there are limits to the purposes for which organisations can collect, use and disclose personal data.

2 The principle of purpose limitation is given effect through the Purpose Limitation Obligation as set out in s 18 of the PDPA, which provides as follows:[3]

> 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 section 20, if applicable.

---

* The author would like to thank Ms Wee Su-ann for her invaluable research assistance. 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.

† Sheridan Fellow, National University of Singapore.

1 Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (adopted on 2 April 2013) at p 4.

2 See Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA") s 3. On the legislative purposes of the PDPA generally, see Benjamin Wong, "Data privacy law in Singapore: the Personal Data Protection Act 2012" (2017) 7(4) *International Data Privacy Law* 287 at 290.

3 Personal Data Protection Act 2012 (Act 26 of 2012) s 18.

3 It is clear from s 18 that there are two requirements relating to the purposes for which an organisation can collect, use, or disclose personal data: the first requirement under s 18(*a*) is that the purposes must be reasonably appropriate; the second requirement under s 18(*b*) is that the individuals concerned must have been notified of the purposes.

4 The primary objective of this article is to clarify the appropriate purpose requirement under s 18(*a*), drawing upon existing guidelines and decisions from the Personal Data Protection Commission ("PDPC"), with reference to foreign jurisprudence where required. The article will first discuss the function and operation of s 18(*a*) in the context of the Singapore data protection regime, before discussing how s 18(*a*) applies in Singapore via a simple two-step analysis.

II. Function and operation

5 The function of s 18(*a*) is to impose a normative standard on organisations when they collect, use and disclose personal data – they can only do so for appropriate purposes. This normative standard is an integral component of a data protection regime that seeks to promote the responsible handling of personal data. It ensures that the processing of personal data is done in accordance with prevailing ethical and social norms, and that both the manner and outcome of data processing "conform with the reasonable expectations" of the individuals affected.[4]

6 Section 18(*a*) functions in tandem with the consent mechanism in the PDPA. The consent mechanism is constituted by the Notification Obligation and Consent Obligation, which respectively require organisations to (a) notify individuals of the purposes for which they are collecting, using or disclosing their personal data, and (b) obtain the individuals' consent for doing so.[5] The consent mechanism thus provides a procedural form of protection to individuals, while substantive protection is conferred by s 18(*a*).

---

4 See Lee Andrew Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) at p 153.

5 See generally Personal Data Protection Act 2012 (Act 26 of 2012) ss 13 and 20.

7 In terms of its operation, it should be emphasised that s 18(*a*) imposes an obligation that is *independent* of notification and consent: an organisation must comply with s 18(*a*) even when it has already obtained valid consent from the relevant individuals.[6] Thus, an organisation cannot collect, use or disclose personal data for an inappropriate purpose, even if the individual concerned has given his or her consent for that purpose. For example, in *Re Galaxy Credit & Investments Pte Ltd* ("*Re Galaxy Credit*"), an organisation was found to have breached s 18(*a*) by its use of a photograph for the purposes of debt collection even though it had obtained valid consent for that purpose.[7]

8 When applying s 18(*a*) to the facts of a particular case, the structure of s 18 suggests the following two-step analytical approach. The first question is whether the collection, use or disclosure is *for* a purpose. Based on the answer to the first question, the second question is whether that purpose is one that a reasonable person would consider *appropriate* in the circumstances. This article will proceed on the basis of this two-step analytical approach.

III. First question: for a purpose

9 As mentioned above, the first question is whether the collection, use or disclosure in question is *for* a purpose. This should be seen as a threshold requirement: if an organisation cannot even point to a purpose that is served by the collection, use or disclosure, then it is necessarily in breach of s 18, and further analysis would be redundant.

10 In two instructive PDPC decisions wherein organisations were found to have breached s 18, the organisations involved appear to have failed to meet this threshold requirement. These two decisions are discussed below.

11 In *Re Universal Travel Corporation Pte Ltd*[8] ("*Re Universal Travel*") four customers of a tour had requested that the respondent provide them with confirmation of the cancellation of their flights, in order for them to process their insurance claims. The respondent duly sent the four customers written confirmation of the flight cancellation. However, the respondent

6 *Re AIA Singapore Private Limited* [2017] PDP Digest 73 at [18].

7 [2019] PDP Digest 288. This case is further discussed below.

8 [2017] PDP Digest 36.

also sent the four customers a full passenger list which contained details of all 37 passengers on the tour. The PDPC found that the disclosure of the full passenger list went "beyond supporting an individual customer's insurance claim", as each individual customer only required his or her own flight details and did not require the details of all the other passengers.[9] Thus, the disclosure of the full passenger list was in breach of s 18.

12 In this case, the claimed purpose of the disclosure (that is, helping a customer process his or her insurance claims) may well have been appropriate. The problem was that disclosing the personal data of other passengers was entirely irrelevant to serving that purpose, hence the disclosure was not "for" that purpose (or indeed, any purpose at all).

13 In *Re AIA Singapore Private Limited*,[10] the respondent was an insurance company who disclosed the complainant's personal data to the complainant's chiropractor. The personal data disclosed included the complainant's bank account details. This was purportedly for the purpose of requesting for a medical report, which the respondent required in order to process the complainant's insurance claim. The PDPC found that the respondent had violated s 18 by disclosing the bank account details to the chiropractor.

14 Here, the bank account details were irrelevant to the chiropractor's role in the claim process and disclosing the bank account details would not facilitate the procurement of the medical report from the chiropractor; no reasonable explanation was provided on why the disclosure needed to be made in the circumstances. Similar to *Re Universal Travel*, the personal data of the complainant in this case was disclosed "without good reason or purpose".[11]

15 The two cases mentioned above make it clear that if an organisation fails to meet the threshold requirement – namely, that its collection, use or disclosure of personal data be "for" a purpose – then it is, without more, in breach of s 18. This threshold requirement is an objective one. If, however, the organisation successfully establishes that the collection, use or disclosure in question does serve a purpose, then the analysis proceeds to the second

9 *Re Universal Travel Corporation Pte Ltd* [2017] PDP Digest 36 at [14].

10 [2017] PDP Digest 73.

11 *Re AIA Singapore Private Limited* [2017] PDP Digest 73 at [19].

question, which requires an assessment of the appropriateness of that purpose.

IV. Second question: appropriateness of purpose

16 Assuming that the threshold requirement discussed above is met, the question then turns to the more substantive question of whether the purpose for the collection, use or disclosure is "appropriate".

17 It should be emphasised at the outset that "appropriateness" must be assessed in the light of the circumstances of the collection, use or disclosure in question, and it cannot be assessed in the abstract. As explained by the Canadian Federal Court in *Eastmond v Canadian Pacific Railway*, "the appropriateness of purposes or why personal information needs to be collected must be analysed in a contextual manner looking at the particular circumstances of why, how, when and where collection takes place".[12] This point is made clear in s 18(*a*) itself, which stipulates that the purpose must be one that a reasonable person would consider appropriate *in the circumstances*.[13] The circumstances that are relevant are those that exist at the time of the collection, use or disclosure.[14]

18 In assessing whether the collection, use or disclosure of personal data has been done for an appropriate purpose, there is no exhaustive list of relevant factors, as all the circumstances of each case should be considered. However, a few factors that are of particular relevance have been highlighted in the existing literature. The PDPC has, in its decisions, provided some guidance as to what factors are of potential relevance in the assessment of appropriateness under s 18(*a*). Guidance may also be drawn from Canadian cases and guidelines relating to similar provisions in Canadian data protection legislation.[15]

---

12 2004 FC 852 at [131].

13 Personal Data Protection Act 2012 (Act 26 of 2012) s 18(*a*).

14 *Wansink v TELUS Communications Inc* 2007 FCA 21 at [15].

15 See Personal Information Protection and Electronic Documents Act (SC 2000, c 5) s 5(3); Personal Information Protection Act (SA 2003, c P-6.5) ss 11, 16 and 19; Personal Information Protection Act (SBC 2003, c 63) ss 11, 14 and 17.

19 Based on a review of the literature, three broad factors may be pertinent, namely: (a) the nature of the purpose, (b) the kind of personal data involved and (c) the manner of the collection, use or disclosure. These factors are well established.[16] The following paragraphs discuss these factors in greater detail.

A. Nature of the purpose

20 The natural starting point for the determination of appropriateness is to assess the quality of the purpose itself. In this assessment, "[t]he purpose should be stated as precisely as possible so that the needs of the organization can be carefully balanced against the rights of the individual".[17]

21 What kinds of purposes are likely to be appropriate? In this regard, it may be questioned whether the collection, use or disclosure of personal data is "directed to a *bona fide* business interest".[18] It may also be asked whether a "legitimate need" was fulfilled by the collection, use or disclosure.[19] These questions should be asked from the perspective of a reasonable person.

(1) Generally appropriate purposes

22 There is a view that purposes listed in the Second, Third and Fourth Schedules of the PDPA are generally thought of as appropriate.[20] There is some sense to this view, as it would have been unlikely for Parliament to

16 A number of overlapping formulations have been adopted by various courts and regulators. These three factors represent a synthesis of these formulations, with a focus on alignment with existing Singapore guidelines.

17 *Order P11-02: Economical Mutual Insurance Company* [2011] BCIPCD 16 at [71]. See also Personal Data Protection Act 2012 (Act 26 of 2012) s 3.

18 *AT v Globe24h.com* 2017 FC 114 at [74]; *Turner v Telus Communications Inc* 2005 FC 1601 at [48], affirmed in *Wansink v TELUS Communications Inc* 2007 FCA 21 at [16].

19 *Eastmond v Canadian Pacific Railway* 2004 FC 852 at [177].

20 Most, but not all, of the exceptions listed in the Second, Third and Fourth Schedules are framed as purposes of collection, use and disclosure, for which consent is not required. The "publicly available" exception is, however, not based upon a purpose (as it relates to the quality of the personal data), and therefore the point made in this paragraph does not apply to it.

have included these purposes as exceptions to the Consent Obligation had it considered these purposes to be generally inappropriate. A similar line of reasoning was taken by the Office of the Information and Privacy Commissioner of Alberta who, in relation to the collection of personal information for the purposes of an investigation or legal proceeding, said that it was "implicit from its inclusion" in the Alberta Personal Information Protection Act[21] ("Alberta PIPA") that this purpose was generally regarded as reasonable.[22]

23 That said, the fact that the purpose of the collection, use or disclosure falls within the Second, Third or Fourth Schedules does not *ipso facto* render it compliant with s 18(*a*). The PDPC has clarified that even where the "*general purpose* of collection, use or disclosure falls within one of the aforementioned exceptions, the *specific purpose* must still be reasonably appropriate" [emphasis added].[23] Thus, for example, although the general purpose of debt recovery may be located in the Schedules of the PDPA,[24] the specific purpose for which the organisation collected, used or disclosed the personal data may still be inappropriate – as would be the case if the organisation used the personal data to threaten violence against the debtor.[25]

(2) Generally inappropriate purposes

24 There are also certain purposes that are generally considered to be inappropriate. In its *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, the PDPC has stated that "a purpose that is in violation of a law or which would be harmful to the individual concerned is unlikely to be considered appropriate by a reasonable person".[26]

---

21 SA 2003, c P-6.5.

22 *Order P2008-008: United Food and Commercial Workers, Local 401* (30 March 2009) at para 98.

23 *Re Club the Chambers* [2019] PDP Digest 304 at [11].

24 See Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule para 1(*i*); Third Schedule para 1(*g*) and Fourth Schedule para 1(*i*).

25 See also *Galaxy Credit & Investments Pte Ltd* [2019] PDP Digest 288 at [11].

26 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 13.4.

25 In a similar fashion, the Office of the Privacy Commissioner of Canada has also set out certain inappropriate purposes or "No-Go Zones", based on its experience in applying s 5(3) of the Personal Information Protection and Electronic Documents Act.[27] These are: (a) unlawful collection, use or disclosure of personal information, (b) profiling or categorisation leading to unfair, unethical or discriminatory treatment contrary to human rights law, (c) collection, use or disclosure for purposes known or likely to cause significant harm to the individual, (d) publishing personal information with the intended purpose of charging individuals for its removal, (e) requiring passwords to social media accounts for the purpose of employee screening, and (f) surveillance through the audio or video functionality of an individual's own device.[28] Although not directly applicable to the PDPA, it is suggested that these "No-Go Zones" are nonetheless useful guidelines to consider.

26 Finally, it is important to note that the PDPC has set out certain guidelines relating to the National Registration Identification Card ("NRIC") in its new *Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers* ("NRIC Guidelines").[29] In essence, under the NRIC Guidelines, there is a limited set of purposes for which organisations can collect, use and disclose NRIC numbers (or NRIC copies) and retain physical NRICs. NRIC numbers or NRIC copies can only be collected, used or disclosed if (a) required under the law, (b) an exception under the PDPA applies, or (c) it is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity; physical NRIC can only be retained if required under the law.[30] It is suggested that this, in effect, means that purposes outside of those listed purposes are generally inappropriate.

---

27 SC 2000, c 5.

28 See Office of the Privacy Commissioner of Canada, *Guidance on Inappropriate Data Practices: Interpretation and Application of subsection 5(3)* (May 2018).

29 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers* (31 August 2018). Note that these rules also apply to other national identification documents: see paras 1.4–1.6.

30 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers* (31 August 2018) at paras 3.1 and 4.1.

B. Kind of personal data involved

27 In considering whether a purpose is appropriate in the circumstances, the kind of personal data being collected, used or disclosed is a relevant circumstance.[31] In particular, account must be taken of the sensitivity of the personal data in question. Certain categories of personal data are regarded as more sensitive, because of the higher potential for harm arising from improper handling of such data.[32] Where sensitive personal data are involved, a greater degree of care should be exercised by organisations, including during the collection, use and disclosure of that personal data.

28 The decision in *Re Galaxy Credit* illustrates the need for organisations to consider the sensitivity of the personal data involved when using personal data. Here the respondent was a licensed moneylender. In the event of default by a borrower, the respondent's practice was to have its debt collectors attach the photograph of that borrower to a letter of demand ("LOD") and leave it in a sealed envelope at the borrower's residence if the borrower was absent. In the present case, the respondent delivered an LOD to a defaulting borrower, but erroneously attached the photograph of another borrower to the LOD, thereby potentially disclosing the indebtedness of that other borrower. The PDPC found that the respondent's practice of attaching a borrower's photograph to their LOD and leaving it at their residence breached s 18(*a*) of the PDPA.

29 A key consideration for the PDPC's finding in *Galaxy Credit* was that sensitive personal data, in the form of information about the indebtedness of an individual was involved. In view of the potential for harm (such as social stigma, discrimination and reputational damage) arising from disclosure of an individual's indebtedness, the respondent should have "exercised greater care in handling this sensitive personal data" and should not have used borrowers' photographs in this way.[33]

---

31 *Order P05-01: KE Gostlin Enterprises Limited* [2005] BCIPCD 18 at [55].

32 See *Re Aviva Ltd* [2018] PDP Digest 245 at [17] for a non-exhaustive list of these categories; see also Benjamin Wong YongQuan, "Protection of Sensitive Personal Data" [2018] PDP Digest 19 at 20–23 for a discussion of the notion of sensitivity.

33 *Re Galaxy Credit & Investments Pte Ltd* [2019] PDP Digest 288 at [17] and [19]. It should be noted that even though photographs of individuals are usually innocuous, the context surrounding the borrower's photograph in this

(*continued on next page*)

C. *Manner of collection, use or disclosure*

30 The manner in which the organisation in question collects, uses or discloses the personal data is also a relevant circumstance. As stated by the Office of the Information and Privacy Commissioner for British Columbia in *Order P09-02: Shoal Point Strata Council*, in determining whether an organisation's purpose is appropriate, the "reasonable person test" considers *how* the organisation handles the personal information in question.[34]

31 The standard here should be that of reasonableness. In other words, when collecting, using or disclosing personal data for a purpose, organisations should do so in a reasonable manner. This is because the standard of reasonableness underpins the PDPA, pursuant to s 11(1).[35] It is also notable that the Office of the Information and Privacy Commissioner of Alberta, in determining whether an organisation had satisfied s 11(1) of the Alberta PIPA, explicitly adopted the criterion of whether the collection was "carried out in a reasonable manner".[36]

32 In *Re Club the Chambers*, the manner of the respondent's collection, use or disclosure of personal data appeared to have played a prominent role in the PDPC's decision.[37] The respondent had put up notices about 11 individuals who were banned from the premises of its computer gaming centre (the "LAN Shop"). These notices included photocopies of the identity documents of the banned individuals, along with remarks explaining why they were banned. The respondent's professed purpose for displaying the notices was to "assist staff in identifying banned members and to inform banned members that they were prohibited entry into the LAN Shop and the reason(s) for the ban".[38] The PDPC nonetheless found

---

case meant that it disclosed sensitive personal data. The importance of context to the assessment of sensitivity is made clear in *Re Credit Counselling Singapore* [2018] PDP Digest 295, in which otherwise innocuous e-mail addresses in a particular e-mail were recognised as sensitive in the light of the content of the e-mail, which sought a status update on the addressees' repayment of their debts.

34 [2009] BCIPCD 34 at [59] and [82].

35 *Re Jump Rope (Singapore)* [2017] PDP Digest 154 at [11].

36 *Order P2006-008: Lindsay Park Sports Society* (14 March 2007) at para 56.

37 [2019] PDP Digest 304.

38 *Re Club the Chambers* [2019] PDP Digest 304 at [14].

that the respondent was in breach of s 18(*a*) of the PDPA.[39] According to the PDPC, while the respondent could not be faulted for wanting to restrict access to certain customers, the *manner* in which the respondent carried out this purpose "left much to be desired".[40]

33 It is suggested that two specific considerations – both of which are also well established in Canadian data protection law – shaped the decision in *Re Club the Chambers*, namely: (a) the effectiveness of the collection, use or disclosure in meeting the organisation's need and (b) the existence of a comparable, less invasive means of achieving the organisation's need.[41] First, on the point of effectiveness, it was clear that if the respondent's purpose in putting up the notices was indeed to identify and exclude certain *persona non grata*, the placing of the notices behind the counter staff "[detracted] from its effectiveness as a blacklist".[42] Second, there was clearly a comparable, less invasive way to achieve the respondent's need to exclude errant customers, and that was through the maintenance of an "internal blacklist", as opposed to putting up public notices for all and sundry to see.[43]

34 A third specific consideration may be the extent to which the collection, use or disclosure results in a loss of privacy to individuals. Support for this specific consideration may be drawn from the decision in *Re My Digital Lock Pte Ltd*, where the PDPC expressed the view that "[i]n determining the appropriateness of any particular purpose, considerations of the data subject's objective expectation of privacy may conceivably be entertained".[44] In this regard, the Canadian courts have adopted a proportionality test, namely whether the loss of privacy is proportionate to the benefit gained.[45] It is respectfully suggested that this proportionality test may not be necessary, as it will suffice to factor any losses to privacy into the broader assessment of appropriateness.

---

39 *Re Club the Chambers* [2019] PDP Digest 304 at [13].

40 *Re Club the Chambers* [2019] PDP Digest 304 at [21].

41 See *Eastmond v Canadian Pacific Railway* 2004 FC 852 at [127]; *Turner v Telus Communications Inc* 2005 FC 1601 at [48]; *Order P13-02: Thyssenkrupp Elevator (Canada) Limited* [2013] BCIPCD 24 at [48].

42 *Re Club the Chambers* [2019] PDP Digest 304 at [22].

43 *Re Club the Chambers* [2019] PDP Digest 304 at [21].

44 [2018] PDP Digest 334 at [39].

45 See for example *Eastmond v Canadian Pacific Railway* 2004 FC 852 at [127].

V. Conclusion

35 In summary, two questions should be asked in relation to any collection, use or disclosure: (a) is it for a purpose, and (b) is that purpose appropriate in the circumstances? The relevant circumstances include (a) the nature of the purpose, (b) the kind of personal data involved, and (c) the manner of collection, use or disclosure. If there is no purpose that a reasonable person would consider appropriate in the circumstances, then the organisation should either avoid the collection, use or disclosure in question, or modify its practices, to be in compliance with s 18(*a*).

36 Section 18(*a*) serves as a necessary complement to the consent mechanism in the Singapore data protection regime, addressing the inherent limits of "notice-and-consent" in protecting the rights and interests of individuals. For instance, it prevents organisations from simply conferring upon themselves *carte blanche* using broad consent clauses.[46] Furthermore, the significance of s 18(*a*) as a component of the Singapore data protection regime may be expected to rise, in the event that more flexibilities are built into the consent mechanism.[47] This article has sought to provide an elaboration on the application of s 18(*a*).

---

46 *Re AIA Singapore Private Limited* [2017] PDP Digest 73 at [18].

47 See Pt II of Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (27 July 2017).

SENSITIVE PERSONAL DATA IN THE SINGAPORE CONTEXT?*

Lanx GOH†
LLB (University of Birmingham), DipSing (National University of Singapore), LLM (Intellectual Property and Privacy Law) (University of California, Berkeley), MSc (Criminology and Criminal Justice) (University of Oxford); CIPM, CIPP/A, CIPP/E, CIPP/US, FIP; Advocate and Solicitor (Singapore); Accredited Mediator (Singapore Mediation Centre and Singapore International Mediation Institute)

Nadia YEO‡
LLB (Hons) (National University of Singapore), Double Masters MPP–LLM (National University of Singapore); Advocate and Solicitor (Singapore); CIPP/A

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views or policy positions of their respective employers. All errors remain the authors' own.

† Team Lead, Investigation Unit (Data Protection and Do Not Call), Personal Data Protection Commission; Adjunct Law Lecturer, Singapore Management University School of Law; and Guest Law Lecturer, National University of Singapore Faculty of Law (will be appointed as Adjunct Assistant Professor from 1 July 2019 onwards). He is also one of the authors for *Data Protection Law in Singapore – Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, 2018) and has spoken at various conferences and seminars such as Data Privacy Asia, IAPP Asia Privacy Forum, IAPP KnowledgeNet and NUS CLE Seminar Series. The author is utmost grateful to Yeong Zee Kin for his patient guidance and invaluable comments. The author would also like to acknowledge Nicholas Fong for proofreading this article.

‡ Deputy Director (Legislation and Policy Advisory), Ministry of Home Affairs. Adjunct Law Lecturer, LASALLE College of the Arts. NUS WYWY Gold Medal Award recipient. She was previously an Assistant Chief Counsel at the Personal Data Protection Commission and is a member of the Law Society's Cybersecurity and Data Protection Committee. The author is indebted to Yeong Zee Kin for his invaluable comments, which helped define the draft to this published version.

I. Introduction

1 The notion that some personal data is more sensitive than others is not a new one in Singapore.[1] In 1990, the Law Reform Committee proposed a data protection framework that distinguished between sensitive and non-sensitive data, by imposing different rules on data users depending on whether or not they deal with sensitive personal data.[2] Later, the 2002 Model Data Protection Code for the Private Sector explicitly granted additional protection to sensitive personal data in its data protection principles.[3]

2 Although the legislative proposals to differentiate between the types of personal data were not carried over by Parliament to the present-day Personal Data Protection Act 2012[4] ("PDPA"), there appears to be tacit recognition by the Personal Data Protection Commission[5] (the "Commission") that some forms of personal data are more sensitive than others.

3 This article examines the recent advisory guidelines and cases decided by the Commission to discern the test used by the Commission in determining what types or categories of personal data are more sensitive than others.

II. Legislative approach to sensitive personal data

4 A preliminary reading of the PDPA suggests that there should be no distinction drawn between the different types of personal data. The PDPA neither defines the term "sensitive personal data" nor distinguishes between

---

1 Benjamin Wong YongQuan, "Protection of Sensitive Data" [2018] PDP Digest 19 at paras 19–28 for an overview of Singapore's approach to dealing with sensitive personal data.

2 Law Reform Committee, Singapore Academy of Law, *Data Protection in Singapore: A Case for Legislation* (Working Paper No 1, 1990) at paras 76–80.

3 National Internet Advisory Committee, *Model Data Protection Code for the Private Sector* (2002) at paras 4.3.4 and 4.7.

4 The Personal Data Protection Act 2012 (Act 26 of 2012) does not differentiate between sensitive and non-sensitive personal data.

5 Section 5(2) of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA") provides that the Personal Data Protection Commission is responsible for the administration of the PDPA.

sensitive and non-sensitive personal data in its imposition of obligations on organisations.

5 In this regard, Singapore's legislative approach to sensitive personal data, while not unique, is different from other jurisdictions like the UK, countries that come within the European Union[6] ("EU") or Malaysia,[7] that have chosen not only to define what constitutes sensitive personal data, but also delineate the categories of personal data that would be regarded as more sensitive or "special".

A. Organisations dealing with sensitive personal data held to more robust standards

6 Yet, the Commission's approach towards applying and enforcing the personal data protection obligations on organisations suggests that there are certain types of personal data that it regards as being more sensitive than others. The Commission is not alone in its approach. Other jurisdictions like Hong Kong,[8] New Zealand[9] and Canada[10] that do not legislate a separate concept of sensitive personal data have similarly introduced the concept into their laws through non-binding guidance and the decisions issued by the respective data protection authorities.

(1) Guidelines

7 In Singapore, the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*,[11] which serve as a supplement and clarification for the obligations in the PDPA, recognise that more stringent or robust measures may be required for organisations to meet their obligations in respect of

6 See Recitals 4, 10, 51, 71, and 75, and Arts 9(1) and 9(2) of the General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018).

7 See ss 4, 6, and 40 of the Personal Data Protection Act 2012 (Act 26 of 2012).

8 See the Personal Data (Privacy) Ordinance 1996 (Cap 486, version 5/04/2013).

9 See the Privacy Act 1993 (No 28).

10 See the Privacy Act 1985 (RSC 1985, c P-21) and Personal Information Protection and Electronic Documents Act 2000 (SC 2000, c 5).

11 Revised 27 July 2017.

sensitive personal data.[12] The *Advisory Guidelines on Enforcement of the Data Protection Provisions*[13] go further in specifying that it would be an aggravating factor for organisations handling sensitive personal data not to have adequate safeguards to protect such data from the harm that may result from its disclosure. [14]

(2) Guides

8 In the same vein, various guides issued by the Commission suggest that different measures may be required when handling sensitive personal data or that organisations may be held to different standards in respect of any such data in their possession or control. For example, the *Guide to Managing Data Breaches*[15] suggests that different notification standards (in respect of timeliness and necessity of communication to the Commission) may apply when dealing with data breaches involving sensitive personal data.[16] The *Guide to Disposal of Personal Data on Physical Medium*[17] suggests that different destruction measures may have to be adopted in respect of sensitive personal data.[18] The *Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data*[19] is rife with references to sensitive personal data and includes similar exhortations for

12 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 17.3, which states that an organisation should "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity".

13 Issued 21 April 2016.

14 Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (21 April 2016) at para 25.2.5.

15 Issued 8 May 2015.

16 Personal Data Protection Commission, *Guide to Managing Data Breaches* (8 May 2015) at p 9.

17 Revised 20 January 2017.

18 Personal Data Protection Commission, *Guide to Disposal of Personal Data on Physical Medium* (revised 20 January 2017) at paras 5.2, 7.3 and 10.4.

19 Issued 20 July 2016.

organisations to use more secure methods and greater caution when processing or sending such data.[20]

9 More recently, the Commission issued a *Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers* which recommended ways for organisations to move away from using NRIC numbers as personal identifiers for individuals. The Commission then took the position that suitable replacement identifiers or combinations of identifiers should not contain "sensitive information" or "sensitive personal information".[21]

10 Thus far, in relation to guides and guidelines, the Commission's approach seems to be premised on a commonsensical approach in terms of the handling of sensitive data. This is notwithstanding the lack of any express definition or categories of such data in the PDPA. In this regard, the next discussion will discern the categories of sensitive data from the Commission's decision. The aforesaid should provide guidance to organisations when it comes to determining whether the personal data in their possession and/or control[22] or processed on behalf of another organisation[23] should be handled with extra care or a higher standard as per the guidelines and guides.

III. Sensitive personal data in the Singapore context?

11 It is imperative to appreciate the fact that there is no common denominator among the various countries when it comes to sensitive data. This is so regardless of whether the jurisdiction has specific legislation dealing with the topic (*eg*, the EU with its General Data Protection Regulation[24] ("GDPR")), or whether the jurisdiction sheds light on the issue via judicial or other authoritative judgments (*eg*, Singapore with the

20 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data* (revised 20 January 2017) at paras 2.1, 2.2, 3.1 and Appendix 1.

21 Personal Data Protection Commission, *Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers* (31 August 2018) at p 4.

22 See s 11(2) of the Personal Data Protection Act 2012 (Act 26 of 2012).

23 See ss 2 and 4(2) of the Personal Data Protection Act 2012 (Act 26 of 2012).

24 (EU) 2016/679; entry into force 25 May 2018.

Commission's decisions). The types of personal data that would constitute sensitive personal data are based on the unique social norms, culture, public expectation and organisation's understanding of a particular country. For example, under the GDPR, the regulation explicitly states that "[t]his Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity".[25] The right to family life is also found in Art 8 of the European Convention on Human Rights 1950. It is without dispute that the GDPR was based on human rights, which in turn reflects the European approach to privacy, *ie*, it arose out of Europe's experiences with personal data being used for the most heinous purposes.[26]

12 However, the PDPA is enacted for economic purposes, *viz*, to enhance Singapore's competitiveness and strengthen its position *as a trusted business and global data hub* by building the trust between consumers and businesses.[27] From past decisions by the Commission, the following types of personal data have been held to affect this trust more severely than others: medical data,[28] financial data,[29] bankruptcy status,[30] drug problem and infidelity,[31] personal data of children[32] and personal identifiers (*eg*, National

25 Recital 4 of the General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018).

26 Olivia B Waxman "The GDPR is just the Latest Example of Europe's Caution on Privacy Rights. That Outlook has a Disturbing History" *Time* (24 May 2018).

27 See *Parliamentary Debates, Official Report* (15 October 2012) vol 89, (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

28 See *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376; *Re Aviva Ltd* [2018] PDP Digest 245 at [18] and Personal Data Protection Commission, *Advisory Guidelines for the Healthcare Sector* (revised 28 March 2017) at para 4.2.

29 See *Re Aviva Ltd* [2018] PDP Digest 245 at [18].

30 See *Re Credit Counselling Singapore* [2018] PDP Digest 295.

31 See *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188.

32 See *Re Singapore Taekwondo Federation* [2019] PDP Digest 247.

Registration Identification Card ("NRIC") and passport details).[33] One reason why such types personal data are considered more sensitive than the others is due to the likelihood and severity of harm in the event of a data breach. In this regard, Benjamin Wong had expounded a harm-based understanding of sensitivity, *viz*, the greater the potential for harm occasioned by its improper collection, use or disclosure, the more sensitive the personal data.[34] This article will expand on his theory and classify the sensitive personal data found in the Commission's decisions into three categories: significant risk of harm, social stigma and objective expectation of privacy. A table fitting the Commission's various decisions into each of the three categories is included for reference. That said, it needs to be noted that the three categories are not mutually exclusive, and in fact many types of sensitive personal data will find themselves fitting into more than one category.

A. Significant risk of harm

13 The idea of risk of harm to an individual is simple. In short, this refers to the fact that unauthorised use or disclosure of data belonging to these categories – for example, financial and medical data; bankruptcy status; personal data of children; information on drug abuse and infidelity; and personal identifiers – is likely to result in significant risk of harm to individuals. For personal identifiers, the *Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers*[35] state that "[g]iven the risks and potential impact of any unauthorised use or disclosure of personal data associated with the individual's NRIC number, organisations are expected to provide a greater level of security to protect

33 Personal Data Protection Commission, *Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers* (31 August 2018) and *Re Singapore Taekwondo Federation* [2019] PDP Digest 247.

34 Benjamin Wong YongQuan, "Protection of Sensitive Data" [2018] PDP Digest 19 at paras 8–12.

35 Issued 31 August 2018.

NRIC numbers (or copies of NRIC) in the possession or under the control of the organisations".[36]

14 To illustrate the point further: NRIC and passport details can lead to the risk of identity theft or fraud.[37] Children might be at risk of being kidnapped or sexually assaulted if their school, address, telephone number, age, *etc,* are made known to strangers. A person might lose his job or marriage if his employer or spouse finds out he has HIV, is bankrupt or has abused drugs in the past. On this note, harm can be physical, social-economic or reputational. In the case of *Re Executive Coach International Pte Ltd*,[38] the Commission noted that the personal data disclosed was highly sensitive and the disclosure was deliberately made to *discredit* the complainant after considering the circumstances. Likewise, the Commission commented that the comprehensive data set in *Re K Box Entertainment Group Pte Ltd*[39] may lead to identity theft, that is, *risk of economic harm*. Last but not least, the *Advisory Guidelines for the Social Service Sector*[40] ("Social Service Guidelines") also state that s 21(3) of the PDPA prohibits the provision of personal data to a person if doing so could reasonably be expected to "cause immediate or *grave harm to the safety or to the physical or mental health* of the individual who made the request" [emphasis added]. In the example provided in the Social Service Guidelines, the son learns about his mother's application for the social service scheme and makes an access request for the personal data that the Social Service has about him, and how it had been used by the Social Service. However, the mother had disclosed to the Social Service that the son was adopted and not her biological son. In this regard, the Social Service can reject the access request as disclosure may cause harm to the mental health of the individual who made the request.

15 Ultimately, what is significant risk of harm will be considered from a reasonable person's perspective,[41] and the cultural and social norms of the

---

36 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers* (31 August 2018) at para 2.4.

37 Hariz Baharudin, "Collecting NRIC numbers and making copies of the identity card will be illegal from Sept 1, 2019" *The Straits Times* (31 August 2018).

38 [2017] PDP Digest 188 at [19].

39 [2017] PDP Digest 1 at [42d] and [43c].

40 Issued 11 September 2014, at para 3.8.

41 See ss 3 and 11(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

society. The harm need not be actual, but is based on whether a reasonable person can foresee that significant harm could potentially result from the data breach. That being said, if there is actual harm established, then it is likely that the Commission will impose a stiffer financial penalty.

B. Social stigma

16 The personal data must carry with it some form of social stigma which is more egregious than mere embarrassment. The concept of social stigma is intertwined with the social norms and culture of a society. For example, gay and lesbian individuals,[42] ex-convicts,[43] HIV-positive individuals (medical data),[44] those who are mentally ill[45] and undischarged bankrupts[46] (financial status) still face certain discrimination in Singapore. This is due to the fact that the majority of the society in Singapore is still by and large conservative.[47] In this vein, individuals might be reluctant to declare their status when applying for jobs,[48] as they run the risk of rejection due to their status.[49]

---

42 See Leow Yangfa, "Various forms of discrimination against LGBTQ individuals reported to support groups" *TODAYonline* (20 September 2018) and Tan Tam Mei, "Shanmugam on India decriminalising gay sex: Singapore society to decide which direction to take" *The Straits Times* (8 September 2017).

43 See Aw Cheng Wei, "He wants to end bias against convicts" *The Straits Times* (1 January 2018).

44 See Janice Lim & Daryl Choo, "HIV-positive individuals still face discrimination despite employment laws to protect them" *TODAYonline* (1 February 2019).

45 See Shirlene Pang *et al*, "Stigma among Singaporean Youth: A Cross-Sectional Study on Adolescent Attitudes Towards Serious Mental Illness and Social Tolerance in a Multiethnic Population" (2017) 7 *BMJ Open*.

46 Evelyn Tan, "Why discriminate against bankrupts?" *The Straits Times* (1 September 2017).

47 Gilaine Ng "55 per cent of Singapore residents still support gay law: poll" *The Straits Times* (11 September 2018).

48 See Janice Lim & Daryl Choo, "HIV-positive individuals still face discrimination despite employment laws to protect them" *TODAYonline* (1 February 2019).

49 Evelyn Tan, "Why discriminate against bankrupts?" *The Straits Times* (1 September 2017).

17 Some of the aforesaid could be argued to carry significant risk of harm as well, although that is not always the case. Harm connotes some kind of economic loss, mental damage or physical injury whereas social stigma is reputational in nature *without a need for harm*, except the threshold is set much higher than mere loss of reputation or embarrassment. For example, financial data is unlikely to bear any social stigma even when disclosed but it can cause financial loss if it results in identity theft.

18 In addition, what is deemed as social stigma today may eventually change over time, *to wit*: the social stigma with drug use is lessening or nonexistent with the younger generation[50] and efforts to tackle discrimination against single mothers by organisations such as AWARE could shift the mindset of society.[51] In short, society's values change with the advancement of civil and human rights, time, technology and education, which in turn define the social stigma of that era.

C. Objective expectation of privacy

19 Personal data where there is an objective expectation of privacy is not dependent on the subjective preferences of individuals. This category basically encompasses personal data which a reasonable person will expect greater protection or care to be taken with respect to the collection, use, disclosure and protection of such data.[52] In this regard, it must be self-evident that a reasonable person would expect his financial and medical data, bankruptcy status or criminal records to be kept confidential. In like manner, the public consultation by the Commission shows the consumers supported the restricted collection, use and disclosure prescribed by the NRIC Guidelines,[53] with parents also being concerned about how their

50 Wong Pei Ting, "The Big Read: Softer attitudes towards drugs a headache for authorities" *TODAYonline* (12 May 2017).

51 See AWARE, "Single Parents" (1 March 2017).

52 See ss 13, 18, 20 and 24 of the Personal Data Protection Act 2012 (Act 26 of 2012).

53 See Infocomm Media Development Authority, "PDPC Issues NRIC Advisory Guidelines to Protection Consumers – Organisations must Implement Changes by 1 September 2019" (10 December 2018).

children's data are used.[54] Both evince an objective expectation of privacy by consumers and parents.

20 From past Commission cases, it can be discerned that people objectively expect privacy to be maintained when there is a relationship, especially one that is fiduciary in nature or where the law imposes confidentiality. Concomitantly, one will expect privacy when it involves a relationship between financial institution or banker and customer, solicitor and client, or doctor and patient. It follows that an objective person will expect details such as beneficiaries of an insurance policy[55] or a will, bank balances[56] or securities holdings,[57] or even a one liner description of a cough or flu, to be treated with higher care even if there is no social stigma and low likelihood of significant risk of harm in the event of a data breach.

IV. Conclusion

21 Based on the above analysis, it appears that the Commission has, through its decisions, provided sound guidance to organisations with regard to the types of personal data that should be handled with greater care. When conducting personal data protection assessments or formulating personal data protection management programmes, organisations should always determine whether the personal data in their possession or control fall within the three categories elucidated. If so, then organisations will be required to exercise due diligence and ensure higher protection throughout the entire life cycle of the personal data, and cease to retain the personal data when there is no longer a business or legal purpose to retain them.[58] Organisations that fail to do so then face the strong possibility of having a harsher financial penalty meted out against them, and loss of consumers' trust.

54 See Daryl Choo, "App popular among school children raises parents' concern over location-tracking function" *TODAYonline* (3 March 2019).

55 See *Re Aviva* [2018] PDP Digest 245.

56 See *Re DataPost Pte Ltd* [2018] PDP Digest 207.

57 See *Re Central Depository (Pte) Limited* [2017] PDP Digest 81.

58 See s 25 of the Personal Data Protection Act 2012 (Act 26 of 2012).

Appendix 1 (selected cases only)

The Commission's decisions	Summary and types of personal data	Classification
Re Central Depository (Pte) Limited and another **[2017] PDP Digest 81**	Data breach due to misalignment of the pages during the sorting process which caused information to be sent to the wrong recipients. Personal data disclosed: a) CDP account information; b) securities holdings; c) transaction summary; and d) payment summary.	Reasonable expectation of privacy for financial data.
Re AIA Singapore Private Limited **[2017] PDP Digest 73**	AIA made an unauthorised disclosure of a customer's personal data, in particular, his bank account details, to Chiropractic First CFP (TP) Pte Ltd. Personal data disclosed: a) name of the bank; b) branch of the bank; c) bank account number; and d) account holder's name.	Reasonable expectation of privacy for financial data.
Re Aviva Ltd **[2017] PDP Digest 107**	Toh-Shi sent out erroneous annual premium statements to Aviva's policy holders. Personal data disclosed: a) names of the policy's dependent; b) sum assured; c) premium amount; and d) type of coverage.	Reasonable expectation of privacy for financial data.
Re Executive Coach International Pte Ltd **[2017] PDP Digest 188**	The organisation's director had disclosed the complainant's past personal history in a WhatsApp group chat comprising the complainant and the organisation's other staff and volunteer trainees. Personal data disclosed: a) name; b) drug problem; and c) infidelity.	Significant risk of harm as individual might lose her job if the employer has issue with hiring someone with a drug problem.

		Both drug abuse and infidelity are likely to cause social stigma in Singapore culture.
Re DataPost Pte Ltd **[2018] PDP Digest 207**	Unintended human error where the operator placed three statements belonging to three individuals into one envelope. Personal data disclosed: a) name; b) address; c) cash balance; and d) type, quantity and valuation of asset holdings.	Reasonable expectation of privacy for financial data.
Re Credit Counselling Singapore **[2018] PDP Digest 295**	The context in which personal data is disclosed may render the personal data sensitive.[59] On the facts, individuals' contact details, which would not ordinarily have been sensitive, were rendered sensitive due to the presence of a follow-up e-mail that had disclosed information regarding the state of indebtedness of each individual.	Significant risk of harm as individual might lose his job if the employer has issue with hiring someone who is a bankrupt. Bankrupt individuals still face social stigma in Singapore culture.

59 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [11]–[16].

Re Aviva Ltd **[2018] PDP Digest 245**	Aviva disclosed personal data without authorisation because it had mistakenly mailed insurance documents belonging to another to one of its policy holders. Personal data disclosed: a) name; b) address; c) policy plan type; d) NRIC number or FIN; e) CPF account number; f) nationality; g) contact number; h) date of birth; i) marital status; j) gender; k) occupation; l) name of employer; and m) name of dependent and his relationship with the policy holder.	Reasonable expectation of privacy for financial data.
Re Aviva Ltd **[2019] PDP Digest 145**	The organisation mistakenly sent out by post underwriting letters meant for three different clients to another client. Personal data disclosed: a) name; b) address; c) medical conditions; and d) sum assured.	Reasonable expectation of privacy for financial and medical data.
Re Singapore Taekwondo Federation **[2019] PDP Digest 247**	The organisation merely collapsed the column in the excel spreadsheet with the NRIC numbers instead of hiding or deleting it. Therefore, the column with NRIC numbers can be replicated despite the fact the original document had been converted into PDF. Personal data disclosed: a) NRIC numbers of children.	Reasonable expectation of privacy for children's personal data.

Re Singapore Health Services Pte Ltd **[2019] PDP Digest 376**	The personal data of some 1.5 million patients and the outpatient prescription records of nearly 160,000 patients were exfiltrated in a cyberattack. Personal data disclosed: a) the names, NRIC numbers, addresses, gender, race, and dates of birth of 1,495,364 SingHealth patients; and b) the outpatient dispensed medication records of 159,000 patients (which is a subset of the full set of illegally accessed personal data).	Reasonable expectation of privacy as involved medical data.

TOWARDS CODES AND CERTIFICATIONS – THE PROTECTION OF PERSONAL DATA IN THE DIGITAL AGE*

LEE Soo Chye†
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore)

TEO Yi Ting Jacqueline‡
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore)

SHEAM Zenglin§
LLB (Hons) (University of London)

I. Introduction

1 Singapore's Personal Data Protection Act[1] ("Act") was enacted on 20 November 2012 and entered into force on 2 July 2014. The stated purpose of the 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".[2] The underlying nature and basis of protection in most of the data protection rules contained in the Act (such as collection, use and disclosure of personal data) is the *rights*

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the legal views or policy positions of their employers. All errors remain the authors' own.

† Senior partner with Aequitas Law LLP. Soo Chye was called to the Singapore Bar in 1990.

‡ Senior associate with Aequitas Law LLP. Jacqueline was called to the Singapore Bar in 2015.

§ Senior legal manager with Aequitas Law LLP. Zenglin graduated from the University of London in 2010.

1 Act 26 of 2012.

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

vested in the individual with regard his or her personal data in the hands of the organisations; such rights take the shape of "consent".[3]

2 With the General Data Protection Regulation[4] ("GDPR") coming into force on 25 May last year, this is an opportune moment to assess the Act and how our data protection rules fare in the face of challenges presented by the rise of the digital age. This paper argues that the effectiveness of "consent", as one of the core pillars of data protection rules, is being drastically eroded. In order to reduce the burden placed on "consent" and to supplement the current "complaints-based" enforcement approach adopted by the Personal Data Protection Commission ("PDPC"), there is an increased need for regulatory intervention which can take the form of data protection safeguards, such as codes of conduct and certification schemes.

II. The erosion of consent

3 In this digital age, the ease of collection of personal data has dramatically increased. Coupled with an exponential growth in the recognition of the value of data and the corresponding creation of business models offering services in exchange for monetising user data,[5] the result is an overload of information and requests for consent. This has inadvertently caused "consent desensitisation" amongst users and consumers, that is, persons agreeing to provide their personal data more readily.[6] In a recent consumer survey on the Act conducted between March and April 2017 by

3 Warren B Chik, "The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy Reform" (2013) 29(5) *Computer Law and Security Review* 554. The author relates the personal data protection principles under the Personal Data Protection Act 2012 (Act 26 of 2012) to the nature of the protection, *ie*, the distribution of duties to organisations and the empowerment of the individual with regard to his or her data in the hands of the organisations. The empowerment of the individual is described by the author as "consent" and "control".

4 (EU) 2016/679; entry into force 25 May 2018.

5 World Economic Forum, "Personal Data: The Emergence of a New Asset Class" (January 2011).

6 Bart W Schermer, Bart Custers & Simone van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16(2) *Ethics and Information Technology* 171.

the PDPC, 73% of the respondents indicated that they would be willing to share personal data in exchange for a benefit such as "discounts, rebates and vouchers", "free products and services" and/or "lucky draws". This percentage had increased steadily since the consumer survey conducted by the PDPC in 2015.[7]

4 While the Act provides that an organisation shall not, as a condition to providing a product or service, require an individual to consent to the collection of personal data,[8] an organisation providing a wide spectrum of services is more often able to craft the scope of the consent obtained from its individual customers in very broad terms to allow the organisation to use the personal data of that individual for very broad purposes. Though never explicitly stated to form part of the terms of service, if the individual does not agree to provide his consent, he will not be able to receive the service. Given the relative unequal balance of economic bargaining power between the individual and organisations, business and commercial reality is such that the individual has little choice but to consent.

5 Against this backdrop, there is mounting criticism of the usage of consent as a meaningful safeguard for data protection. Regulatory intervention appears to be unavoidable and must be thrust into the limelight in the realm of data protection rules. In Singapore, this is evident in the prohibition by law of the rampant practice of indiscriminate collection of NRIC details by organisations, taking effect from 1 September 2019.[9] With the Singapore Government moving towards the vision of building Singapore as a "Smart Nation"[10] and positioning itself as a data

---

7 Personal Data Protection Commission, "Consumer Survey on the Personal Data Protection Act: September 2015"; Personal Data Protection Commission, "2016 Consumer Survey on the Personal Data Protection Act (PDPA)"; Personal Data Protection Commission, "2017 Consumer Survey on the Personal Data Protection Act (PDPA)".

8 Personal Data Protection Act 2012 (Act 26 of 2012) s 14.

9 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers* (31 August 2018).

10 Singapore's Smart Nation initiative was launched by Prime Minister Lee Hsien Loong on 24 November 2014. There will be a wealth of data generated by the Smart Nation initiative with an array of Internet-enabled gadgets:

(*continued on next page*)

hub,[11] it becomes even more crucial for the effectiveness of our data protection laws to be heightened.

III. Shifting focus on regulating organisations – Codes and certification

6 The PDPC currently implements a "complaints-based" approach in the enforcement of data protection laws.[12] While endowed with powers of audit, the PDPC's role was not contemplated to involve active audits of organisations or the certification of compliance to data protection laws. Be that as it may, not all data breaches are discoverable or, even if they are discoverable, reported by organisations. According to the "CyberArk Global Advanced Threat Landscape Report 2018: The Business View of Security", 50% of the respondents stated that their organisations did not fully inform customers when their personal data was compromised.[13] Facebook failed to disclose the Cambridge Analytica data breach until after it was publicly disclosed by a whistle-blower.[14] Uber concealed a cyberattack that resulted

---

Tan Teck Boon, "In Smart Nation drive, S'pore must strengthen personal data protection" *TODAYonline* (2 March 2016).

11 Economic Development Board Singapore, "How Singapore plans to become Asia's big data hub in 2018" (30 January 2018). Facebook and Google have announced investments in data centres to be located in Singapore. See also Jacquelyn Cheok, "Facebook to build S$1.4b data centre in Singapore, its first in Asia" *The Business Times* (6 September 2018); Ann Williams, "Google investing $476m to build third data centre in S'pore" *The Straits Times* (2 August 2018).

12 Ministry of Information, Communications and the Arts, "Public Consultation on the Proposed Personal Data Protection Bill" (19 March 2012) at para 2.125 <https://www.mci.gov.sg/public-consultations/public-consultation-items/public-consultation-on-the-proposed-personal-data-protection-bill?page=1> (accessed 21 April 2019).

13 CyberArk, "CyberArk Global Advance Threat Landscape Report 2018: The Business View of Security" (2018).

14 Erik Larson & Daniel Stoller, "Facebook Faces Intensifying Pressure from Washington on Privacy" *Bloomberg* (20 December 2018) <https://www.bloomberg.com/news/articles/2018-12-19/facebook-sued-by-d-c-over-cambridge-analytica-data-scandal> (accessed 21 April 2019).

in the theft of the data of 57 million customers.[15] In Singapore, more than 14,200 people with HIV had their personal data leaked online around 2013, but the data breach was only made public in 2019.[16] This poses serious consequences and calls into question whether a "complaints-based" approach is effective in ensuring compliance by organisations with data protection laws in the longer term, even more so in the present climate. Along with proposed new changes contemplated in a recent public consultation initiated by the PDPC that will mandate organisations to notify individuals whose personal data have been compromised,[17] it is also necessary to consider moving towards an "audit-based" approach by means of codes and certifications, which the paper will elaborate on below.

A. Enacting codes of data governance

7 The concept of codes of data governance is no stranger to the data protection scene. Off the shores, the GDPR and its predecessor Directive 95/46/EC ("Data Protection Directive") strongly advocate the drawing up of codes of conduct. However, under the Data Protection Directive, codes of conduct need not be approved by a supervisory authority who will merely opine on the codes drawn up.[18] Locally, there are a few codes of practice developed by industry associations which the PDPC had opined on.[19] The PDPC's current approach towards codes of conduct mirrors that required under the Data Protection Directive.

8 The GDPR has climbed one rung higher since the days of its predecessor. Codes of conduct feature much more prominently in the GDPR than in the Data Protection Directive and are a vital component of

15 Eric Newcomer, "Uber Paid Hackers to Delete Stolen Data on 57 Million People" *Bloomberg* (22 November 2017).

16 Claudia Chong, "2nd major breach may further dent Singapore's data hub push" *The Business Times* (29 January 2019).

17 Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy" (1 February 2018).

18 Data Protection Directive (Directive 95/46/EC) Art 27.

19 The Personal Data Protection Commission has opined and made suggestions on the published industry-led codes of practice prepared by the Life Insurance Association of Singapore.

regulating data protection. The GDPR sets out the clear objective to be achieved by codes of conduct, *ie*, they are anticipated to contribute to the application of the GDPR by taking into account the *specific* features of various processing sectors and needs of micro, small and medium enterprises.[20] It further prescribes suggested areas for such codes to govern, such as fair and transparent processing, legitimate interests, collection of data, pseudonymisation of personal data, disclosures to the public, exercise of rights of data subjects, processing of personal data of children, security measures in data processing, breach notifications, international data transfers and dispute resolution processes.[21]

9 Codes of conduct under the GDPR are envisaged to be drafted by private associations who are urged to "consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations",[22] and thereafter submitted to a supervisory authority and further reviewed by the European Data Protection Board and the European Commission where the code relates to processing activities across member states.[23] The adherence to an approved code of conduct would be taken into consideration in the case of an enforcement measure against an organisation for a breach of the GDPR.

10 Although codes of conduct have evidently been recognised as valuable tools to assist organisations with complying with data protection laws, it is unfortunate that both home and abroad, they remain as *optional* tools at the disposal of organisations. The dearth of codes in Singapore, with only two published to date,[24] is a clear indication that developing and optimising usage of codes as a means of compliance is not a matter of priority to organisations. Currently, organisations are reliant on the assortment of

20 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Art 40(1).

21 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Art 40(2).

22 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Recital 99.

23 General Data Protection Regulation ((EU) 2016/679, entry into force 25 May 2018) Arts 40(5)–40(7).

24 The two published codes of practices and conduct are prepared by the Life Insurance Association Singapore.

main advisory guidelines issued by the PDPC ("PDPC Guidelines") complementing the Act. However, these PDPC Guidelines are intended to indicate "the manner in which the [PDPC] will interpret provisions of the [Act]". While the PDPC's efforts in publishing the guidelines are commendable, the shortcoming of the PDPC Guidelines is that they are expressed to be purely advisory in nature – organisations are still required to seek legal advice, and the PDPC Guidelines are subject to change at the PDPC's absolute discretion.[25]

B. Certification through a Data Protection Trustmark

11 In contrast to codes, certification is a new player in the data protection scene. The notion of certification was introduced in the GDPR, which envisages the accreditation of certification bodies and the establishment of approval criteria for certification.[26] The GDPR also boosted the value of certification by, amongst others, enabling the certification to be utilised as a means to demonstrate compliance and as a legal ground for transfer of personal data to countries outside the European Union.[27] Shortly after the GDPR came into force, in Singapore, the PDPC launched the Data Protection Trustmark ("DPTM") Certification to be administered by the Info-communications Media Development Authority. The DPTM is intended to be a "visible indicator that an organisation adopts sound data protection practices".[28] The certification requirements are based on parameters including relevance to international data protection standards and industry best practices.

12 Still in its initial stage of implementation, certification is a *voluntary* process that organisations may choose to undertake. Pending the demonstration of positive results on the effectiveness of certification schemes, it is understandable that regulatory bodies are hesitant to impose it as a mandatory obligation on organisations. Yet, results can only show when more organisations participate. The participation rate of organisations in

25 Personal Data Protection Commission, "Introduction to the Guidelines".

26 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Art 43.

27 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Art 46(2)(f).

28 Personal Data Protection Commission, "Data Protection Trustmark".

the DPTM Certification scheme is low, with only nine organisations obtaining a DPTM since the scheme was launched in July last year as at 29 April 2019.[29]

13 It must be recognised that certification, as a form of regulatory intervention, can play an imperative role in safeguarding the protection of personal data, not just in making certain that organisations comply with relevant data protection rules. Where obtaining certification becomes a norm for organisations, this can contribute to a change in attitudes and perception of business leaders towards data protection in this digital age and increase their cybersecurity awareness. However, a considered exercise must be carried out to balance the need to protect personal data and the business demands and cost constraints faced by an organisation. The costs of certification can arguably put a strain on some organisations, particularly small and medium enterprises.[30] Such costs, including compliance costs, must be weighed against how much society regards the importance of protection of personal data in the digital age.[31]

---

29 Infocomm Media Development Authority, "List of DPTM-Certified Organisation" (29 April 2019).

30 Infocomm Media Development Authority, "Data Protection Trustmark Certification" (2 April 2019). In order to obtain the Data Protection Trustmark which has a validity period of three years, the fees for application and assessment range from $2,000 to $10,000, depending on the size of an organisation.

31 An example can be found in the measures taken to combat money laundering activities imposed by the Accounting and Corporate Regulatory Authority. The key personnel of registered filing agents ("RFAs") must attend certification courses relating to anti-money laundering courses as a requirement to be registered as RFAs to provide corporate secretarial services. While such certification and compliance will add to business costs, when weighed against the need to ensure that businesses are not complicit in enabling money laundering activities to take place, the latter need prevails. All RFAs, whether they are big and small organisations, must undergo such certification given that it is imperative that money laundering activities do not take root in Singapore.

IV. Codes and certification as the way forward

14 Given the challenges of technological advancements, the writers' view is that it is now imperative to re-calibrate the original premise on which the current PDPA was drafted.[32] It is time to consider a position where an organisation which processes personal data in the course of its business is required to undergo a mandatory certification process by which its adherence to a code of practice applicable to its industry is verified, and such certification will have to be renewed at regular intervals. If an organisation does not wish to undergo the certification process, then its management must declare that the organisation shall not process personal data in the course of its business. Weighed against the cost of compliance, if society truly regards personal data to be of such value that it must be protected, more so considering the ease of collection as a result of technological advances in the digital age, the rules and regulations should adequately reflect the value that society places on personal data. A business that chooses to organise itself such that it needs to process personal data must be prepared to absorb compliance costs in order to abide by codes and obtain certification. Clear rules and regulations will serve to promote an environment where technological advances can be appropriately harnessed by businesses.[33]

15 To be sure, the initiative of the Life Insurance Association of Singapore to develop its own codes of data governance with input from the

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

33 In this regard, it is commendable that even while advances in artificial intelligence ("AI") and the exploitation of new technology are at a nascent stage, the Personal Data Protection Commission ("PDPC") has taken steps to put forward a "proposed accountability-based framework" to provide common definitions and a common structure to facilitate constructive and systematic discussions on ethical, governance and consumer protection issues relating to the commercial deployment of AI. The PDPC also encourages businesses to use the framework for internal discussion. Trade associations and chambers, professional bodies and interest groups are welcome to use this document for their discussion and encouraged to adapt it for their own use. See also Personal Data Protection Commission, "Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI" (5 June 2018) at p 2.

PDPC is already a right step in this direction.[34] This practice can be fostered by building up codes from the existing sector-specific industry guidelines prepared by the PDPC in close collaboration with industry players. It is anticipated that the list of codes will expand with more direct regulatory involvement. Codes of data governance should eventually become a key tool for all organisations processing personal data in observing data protection laws. In implementing this new paradigm, it may also be essential to require all organisations, whether big or small, to be part of an industry or sector-specific association,[35] and necessitate each association to develop a code of data governance specific to the business needs of that industry.[36] In this way, all businesses would be able to abide by a suitable

34 See Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy" (1 February 2018).

35 The requirement for all businesses to be part of an association or similar corporate body is not new. All companies with paid-up capital of $500,000 or more are required to be a member of the Singapore Business Federation. Members are required to pay an annual fee ranging from $300 to $800 depending on their paid-up capital. For non-profit organisations, where they are carrying out charitable purposes, they are required to be registered under the Charities Act (Cap 37, 2007 Rev Ed) and abide by the code of governance issued by the Commissioner of Charities. Businesses that do not wish to operate within this paradigm may choose to declare that they will not collect personal data in their business operations, in which case the codes developed by their industry will not apply to them.

36 The recent approach taken by the Singapore Exchange Limited ("SGX") to incorporate principles in the Code of Corporate Governance ("CCG") for listed companies into its Listing Manual may be instructive on the approach to take in ensuring compliance with principles of data governance by organisations handling significant personal data. Whereas the general approach in the Listing Manual to ensure compliance by listed companies with the CCG has been to require the listed companies to "comply or explain" in their annual reports the extent of compliance with the CCG, the Listing Manual has recently been amended to specifically incorporate the principle in the CCG on the issue of whether a director is considered an independent director. The effect of this amendment is that with effect from 1 January 2022, in order for a listed company to maintain its listing status on SGX, it no longer is merely able to explain any non-compliance with this principle in its annual report; it will be mandatory for the listed company to comply with the principle as part of its continuing listing obligations. It is the writers' hope that

(*continued on next page*)

code of data governance, ensuring consistent conformity to data protection laws across organisations.

V. Concluding thoughts

16 With the erosion of consent, it appears inevitable that regulatory intervention in the form of codes and certification is necessary in order to keep the walls guarding our personal data standing tall against the waves of fast-moving developments in the digital age. This is especially so when individuals are in no position to protect themselves against the likes of technology giants like Facebook, Google, Grab and Alibaba, and big commercial organisations such as banks and financial institutions. It is hoped that with increased regulatory intervention to protect personal data, an environment of trust from consumers will be developed, thereby allowing lawful businesses to harness the fast-paced changes in the digital world for the benefit of the consumers in the longer run.

---

as clear sector-specific principles (*ie*, codes) are developed for organisations within their industry sectors for data governance, organisations will adhere to the codes of their specific sectors and there will be no need for regulatory intervention.

PROCESSING PERSONAL DATA BASED ON LEGITIMATE INTERESTS: A PARADIGM SHIFT*

Charmian AW†
LLB (Hons) (National University of Singapore);
CIPP/A, CIPP/E, CIPP/US, CIPM, FIP; Advocate and Solicitor (Singapore)

Cynthia O'DONOGHUE‡
BA (Arizona State University), LLM (University of Edinburgh),
JD (University of California, Davis School of Law);
Solicitor (England & Wales and Ireland); Member (New York Bar)

I. Introduction

1 Since the advent of the Personal Data Protection Act ("PDPA") in 2012, there have been a number of significant developments as well as announcements made as to its future amendments.[1] One such change that has been announced is the proposed introduction of a legitimate interests basis for processing personal data that does away with the need for individual consent. In fact, such basis already exists under the European Union's General Data Protection Regulation ("GDPR"), which came into effect on 25 May 2018. This article seeks to examine this particular ground for processing personal data and provide a comparative look at the GDPR – the rationale/purpose of the doctrine, as well as its applicability – which will hopefully aid in formulating a more holistic understanding of the forthcoming amendment to Singapore's law.

---

* Any views expressed in this article are the authors' personal views and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Counsel, Reed Smith, Singapore.

‡ Partner, Reed Smith, London.

1 See "Public Consultations" *Personal Data Protection Commission* <https://www.pdpc.gov.sg/Legislation-and-Guidelines/Public-Consultations> for a list of public consultations to date.

II. Analysis of the legitimate interests basis of processing personal data under the General Data Protection Regulation

A. Wording of the General Data Protection Regulation

2 The GDPR allows for the lawful provision of personal data where the processing is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party".[2] There is limited explanation in the GDPR about what this covers; however, the GDPR does state that a legitimate interest could exist where there is a "relevant and appropriate relationship between the data subject and the controller", for example where "the data subject is a client or in the service of the controller".[3]

B. Rationale/purpose of the doctrine under the General Data Protection Regulation

3 The legitimate interests basis pre-dates the GDPR. The GDPR does not fundamentally alter the concept of legitimate interests compared to the Data Protection Directive 95/46/EC ("DP Directive") or the UK's Data Protection Act 1998,[4] but it does introduce a higher threshold.

4 The legitimate interests basis is flexible, and facilitates the day-to-day running of business, including protecting businesses from onerous obligations. Without this legal basis, businesses could be faced with the onerous task of having to obtain consent from a data subject who already reasonably expects that such processing will occur. Allowing businesses to circumvent this obligation means they are able to save both time and money.

5 Further, the legitimate interests basis allows businesses to exercise more long-term control over their processing activities, without fear of individuals withdrawing consent at any time, which could be disruptive to the business.

---

2 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Art 6(1)(f).

3 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Recital 47.

4 c 29.

6 The flexibility of the legal basis also provides a benefit to data subjects: data subjects are spared the hassle of being asked to provide consent for data processing which they already reasonably expect will occur and are unlikely to object to.

7 Giving businesses this freedom is possible without much controversy since the legal basis is somewhat "self-regulatory". In order to rely on the legal basis, the business must satisfy itself that the legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject. Under the old regime, the threshold was lower, requiring that such processing does not "prejudice" an individual's rights and freedoms. The GDPR thus moves away from the narrow harm-based assessment, towards a wider concept of protection.

8 A significant limitation of the legitimate interests basis is that it does not cover processing by public authorities in the performance of their tasks as a public authority.[5] This is because the processing of personal data for the performance of these tasks should only be done with authority given by the law.

C. *Applicability of the legitimate interests basis*

9 In order to determine whether the legal basis applies, the Information Commissioner's Office in the UK ("ICO") has suggested that the controller ask itself three questions:[6]

(a) Purpose: are you pursuing a legitimate interest?
(b) Necessity: is the processing necessary for that purpose?
(c) Balancing: do the individual's interests, rights and freedoms override the legitimate interest?

10 "Legitimate interests" covers a wide array of interests. It covers the interests of the controller or any third party; commercial interests or wider societal benefits; and compelling interests or merely trivial interests.

---

5 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Recital 47.

6 UK Information Commissioner's Office, "Legitimate Interests" (22 March 2018) at p 3 <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf> (accessed 18 April 2019).

11 The GDPR does not prescribe what interests are "legitimate", or the facts to be taken into account when determining this. The GDPR does, however, suggest activities that may indicate a legitimate interest, namely: processing employee or client data, direct marketing, or administrative transfers within a group of companies.

12 The question of "necessity" is satisfied by demonstrating that the processing is targeted and proportionate for achieving the purpose. Consideration must be given to whether there is a less intrusive alternative. This is where a strong, clearly defined purpose for the processing will be essential.

13 The legal basis cannot be relied on if the interests and fundamental rights of the data subject override the legitimate interests. Therefore, organisations must ensure that such interests are weighed up against each other. This balancing exercise is necessary because, unlike other bases for lawful processing, legitimate interests is not focused on a particular purpose, nor does it presume a data controller's interests are aligned with the interests of the data subject.

14 "Interests and fundamental rights" is broad and extends further than just data protection and privacy rights. The ICO suggests that interests and fundamental rights may override legitimate interests if the individual cannot reasonably expect the processing to occur, as this could be evidence of the individual having lost control over the use of his data. Reasonable expectations can be affected by how long ago the data was collected, the source of the data, and the relationship between the controller and data subject.

D. Comment

15 The legitimate interests legal basis interacts with other requirements in the GDPR, chiefly accountability and transparency. Entities must be able to identify what the legitimate interests they rely on are and document the decision-making, including the factors taken into account.

16 Generally, legitimate interests can be an appropriate basis for processing where: there is limited privacy impact; processing is not required by law but confers a clear benefit to the organisation; and individuals could reasonably expect their data to be used in such a way.

III. Key takeaways for Singapore

A. Personal Data Protection Commission's response to the public consultation on managing personal data in a digital economy

17 In its public consultation on approaches to managing personal data in the digital economy on 27 July 2017,[7] the Personal Data Protection Commission ("commission") noted the importance of data for innovation and growth whilst expressly acknowledging that in today's digital economy, unprecedented challenges have been presented to consent-based approaches to personal data protection.

18 For instance, as it would not always be possible for an organisation to anticipate the purposes for using personal data at the outset, it may be unable to seek consent in every instance of data collection, or to attempt to identify the individuals to seek their consent for each new purpose. The facilitation of withdrawals of consent could also pose a significant challenge. In addition, relying only on consent could lead to undesirable effects such as organisations resorting to obtaining consent through lengthy or broadly worded notices, thereby leading to consent fatigue.[8]

19 Against this backdrop, it was recognised that alternative approaches that calibrate the balance of responsibilities by holding organisations accountable to act responsibly and adopt pre-emptive preventive measures could help meaningfully address such issues. More specifically, the commission felt that there was a need to strengthen provisions for *parallel* bases for collecting, using and disclosing personal data under the PDPA, to cater to circumstances where consent is neither feasible nor desirable, and where such collection, use or disclosure would benefit the public (or sections thereof).[9]

20 One such basis proposed by the commission is where an organisation has legitimate interests in processing personal data. In his keynote speech at

---

7 Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (27 July 2017).

8 Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (27 July 2017) at paras 2.2–2.3.

9 Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (27 July 2017) at para 3.3.

the Peking University Law School and Development Academy on 15 January 2019, Data Protection Advisory Committee Executive Chairman Leong Keng Thai remarked that:[10]

> 12 To ensure that the regulatory environment keeps pace with evolving technology in enabling innovation, the Commission is reviewing the Act and has to date conducted two rounds of public consultations to gather feedback on our proposed changes.
>
> 13 As I have stated before, we cannot rely on consent to be the only control on how personal data is used. We need to enhance our consent regime by introducing parallel bases for processing personal data …
>
> 14 There may be other times when the larger interests of systemic benefits override individual preferences. One clear example is monitoring payment transactions for fraudulent activities or money laundering attempts. The need to maintain systemic integrity and trust will trump individual's preferences. I should also add that oftentimes, it is the crooks who will withhold consent if they know that someone is watching! We are therefore introducing legitimate interest as a way to allow organisations to make use of data without having to obtain consent when there is a larger benefit to society.

21 However, when relying on the legitimate interests basis, greater responsibility would be required from organisations to demonstrate their accountability in safeguarding the personal data of individuals.

22 In its public consultation paper on approaches to managing personal data in the digital economy,[11] the commission further cited the GDPR as having a similar basis for processing personal data without the need for consent, wherein the individual's fundamental rights to personal data protection are weighed against possible legitimate interests of the organisation, including enforcing a legal claim, preventing fraud, monitoring employees for safety or management purposes, and conducting scientific research. The GDPR also highlights certain processing activities where the legitimate interests basis is "*likely*" to apply; namely, with the

---

10 See "Keynote Speech by DPAC Executive Chairman, Mr Leong Keng Thai, at the Peking University Law School & Development Academy on Tuesday, 15 January 2019 in Beijing, China" *Personal Data Protection Commission* (15 January 2019).

11 Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (27 July 2017) at para 3.12.

processing of employee or client data, direct marketing or intra-group administrative transfers.

23 In its response to feedback on the public consultation on 1 February 2018,[12] the commission reiterated that there are circumstances in which organisations may need to collect, use or disclose personal data without consent for a legitimate purpose but this is not authorised under the PDPA or other written laws; for instance, with the sharing and use of personal data to detect and prevent fraudulent activities. This should be contrasted against non-legitimate interests such as an organisation's direct marketing purposes. The PDPC clarified that the main intent of the legitimate interests basis would be to enable organisations to protect their legitimate interests in so far as these have an economic, social, security or other benefit for the public (or a section thereof), and where it is not feasible to obtain individuals' consent in the relevant circumstances (again, to avoid fraud detection, for instance).

24 Hence, the PDPC affirmed the need to provide for a legitimate interests basis for processing, and further clarified that it will retain, with rephrasing to the extent as may be appropriate, "the condition that 'benefits to the public (or a section thereof) must outweigh any adverse impact to the individual' as part of the accountability measures to be implemented by organisations" relying on this basis for processing.[13]

25 In particular, organisations will need to conduct a risk and impact assessment to determine whether the benefits outweigh any foreseeable adverse impact to the individual. With regard to this requirement, it is hoped that additional clarification or guidance will be issued in due course on how this assessment may be conducted; for example, as an update to the PDPC's *Guide to Data Protection Impact Assessments* issued on 1 November 2017.[14]

---

12 Personal Data Protection Commission, *Response to Feedback on the Public Consultation Approaches to Managing Personal Data in the Digital Economy* (1 February 2018) at paras 5.1 and 5.7.

13 Personal Data Protection Commission, *Response to Feedback on the Public Consultation Approaches to Managing Personal Data in the Digital Economy* (1 February 2018) at para 5.8.

14 Personal Data Protection Commission, *Guide to Data Protection Impact Assessments* (1 November 2017).

26 Such risk and impact assessment will also need to be *documented* by the organisation. At the same time, the PDPC took on board industry feedback to the consultation that there could be potential commercial sensitivity in respect of such assessments, and hence it clarified that the assessment need not be made available to the public or individuals on request, but rather should only be disclosed to the commission where the commission is determining whether there has been a contravention of the PDPA.

27 Additionally, an openness requirement[15] will be imposed such that the organisation will need to disclose its reliance on the legitimate interests ground for processing personal data (for instance, via its data protection policy that is made available to the public), and make available a document justifying its reliance on the legitimate interests ground, and the business contact information of its data protection officer. This mirrors the accountability requirement under the GDPR, where reliance and decisions based on legitimate interests need to be similarly documented.

B. Potential impact of new basis for processing on Singapore

28 Legitimate interests is often considered as the most flexible of the six lawful bases[16] for processing personal data under the GDPR.[17]

---

15 Personal Data Protection Commission, *Response to Feedback on the Public Consultation Approaches to Managing Personal Data in the Digital Economy* (1 February 2018) at para 5.9.

16 The others comprise consent, contract, legal obligation, vital interests and public task. Consent is where the individual has given clear consent for his personal data to be processed for a specific purpose. Contract is where the processing is necessary for a contract with the individual, or at the individual's request. Legal obligation is where the processing is necessary for the organisation to comply with the law. Vital interests is where the processing is necessary to protect someone's life. Public task is where the processing is necessary for the organisation to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

17 See, for instance, UK Information Commissioner's Office, "Legitimate Interests" (22 March 2018) at p 22 <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf> (accessed 18 April 2019).

29 The exact impact and implications of this new basis for processing personal data on Singapore remain to be seen. Nonetheless, these could potentially be far-reaching. We discuss a couple of examples briefly here.

(1) Whose legitimate interests?

30 Firstly, the issue could arise as to *whose* legitimate interests should be taken into account when relying on the legitimate interests basis for processing personal data. It is most appropriately used when:

(a) the processing is not required by law but has a clear benefit to the organisation or others;
(b) there are minimal identified risks *vis-à-vis* the individual(s) and these risks can be addressed by appropriate measures;
(c) the individual(s) would reasonably expect that their personal data will be used in that way; and
(d) the organisation cannot or does not want to give the individual(s) full upfront control with consent, provided that they are unlikely to object to the processing.

31 In the EU, a business can process personal data where this is necessary for purposes of legitimate interests pursued by the business itself or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

32 In an opinion concerning Fashion ID and Facebook issued on 19 December 2018,[18] the European Court of Justice Advocate General ("AG") considered the parties' status as joint controllers under the DP Directive. Fashion ID's website inserted Facebook's "Like" button as a plug-in, allowing personal data, such as the user's IP address and browser journey, to be transferred to Facebook regardless of whether the user clicked on the Facebook "Like" button. A consumer protection association brought a claim against Fashion ID, arguing that the use of the Facebook "Like" button was a breach of data protection laws.

33 The AG proposed that both Fashion ID and Facebook be considered joint controllers of the personal data. Fashion ID is a joint controller as it caused the collection and transmission of user personal data by inserting the

18 C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*.

plug-in. However, both parties "co-decide on the means and purposes of the data processing at the stage of the collection and transmission of the personal data".[19]

34 Accordingly, both parties' legitimate interests should be taken into account, and these would then need to be balanced against the rights of the individuals concerned.

(2) Potential distinctions between the approaches in Singapore and the European Union

35 There appear to be at least two distinctions between the proposed approach in Singapore and that in the EU.

36 Firstly, it would appear that the balancing of interests in Singapore would be that of the public's and whether there is any adverse impact or risk posed to the individual; whereas in the EU it would be whether the business or a third party's legitimate interests are overridden by the data subject's interests, rights or freedoms.

37 Secondly, the legitimate interests exception, along with the notification of purpose basis for processing personal data which the commission also proposed to introduce in its response to the public consultation, would provide new avenues for businesses to process personal data without the need for consent. Whilst commercial businesses in Singapore would have typically sought to rely on consent to date, whether they continue to do so will depend on the type of processing they intend to carry out as well as the purposes of such processing. Existing practices and procedures may therefore need to be reviewed and revised accordingly.

(3) Departure from consent and the movement towards a risk and impact assessment approach

38 Crucially, such departure from a consent-based regime will likely lead to an increased emphasis on the risk and impact assessment approach to data protection in Singapore. It remains to be seen what kinds of scenarios would be considered as bringing about benefits to the public or a section

19 C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* at [106].

thereof, as well as when these "clearly outweigh" any adverse impact or risks to the individual.

39 However, if for any reason an organisation cannot offer people a genuine choice over how their data may be used, then consent will likely not be an appropriate basis for processing. This may be the case if, for example, an organisation would still need to process the data if consent were refused or subsequently withdrawn, or if it has a position of power over the individual (*eg*, an employer processing employee data, *etc*).

IV. Conclusion

40 It can be expected that the commission will, through advisory guidelines and other resources to be issued in due course, provide further clarification on the applicability of the legitimate interests ground of processing personal data, so as to guide organisations on how to comply with the PDPA when seeking to rely on it. Areas in which more detailed guidance is desired may include the circumstances that may bring about benefits to the public or a section thereof, what needs to be undertaken in respect of the risk and impact assessment, whether and how organisations may rely on legitimate interests for the processing of minors' personal data, as well as for marketing purposes, amongst others.

ARTIFICIAL INTELLIGENCE AND THE PERSONAL DATA PROTECTION ACT*

LIM Jeffrey, Sui Yin
LLB Hons (Bristol University);
Advocate and Solicitor (Singapore), Barrister-at-law (England & Wales)

I. Introduction

1 We are at an inflexion point in legal thinking on artificial intelligence ("AI") matters. Regulators and other interested stakeholders in many parts of the world are addressing the content, role and scope of regulation needed to address the impact of AI.[1]

2 The discussions taking place on AI address many aspects, but one major theme concerns the impact that the development and application of AI technology will have on issues of data protection (and privacy).[2] It is in this context that the Personal Data Protection Commission ("PDPC") issued a discussion paper on AI and personal data (the "PDPC AI Paper")

---

* 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.

1 Since June 2018, the Infocomm Media Development Authority has been engaging key stakeholders (including the Government, industry, consumers and academia) to drive awareness of the benefits and understand the challenges, ethics and legal issues of artificial intelligence ("AI"). There are three new structured, interlinked initiatives which are in place or have been executed to accomplish this, namely: an Advisory Council on the Ethical Use of AI and Data, the publication of the "Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI", and a research programme on the governance of AI and data use to advance and inform scholarly research on AI governance issues.

2 There are important differences between concepts of privacy and data protection. For an example of how these two concepts can diverge, seen from a jurisdiction where concepts of privacy and data protection exist, see Juliane Kokott & Christoph Sobotta, "The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR" (2013) 3(4) *International Data Privacy Law* 222.

on 5 June 2018, and further tabled for voluntary adoption, and for feedback by 30 June 2019, the Proposed Model Artificial Intelligence Governance Framework (the "Model Framework"). As Singapore considers what shape its regulatory framework should take in this regard, it is useful to take stock of the country's existing data protection laws and how they could inform the development of such regulations.

3 This paper will discuss how data protection will often be a feature in AI solutions even where there has been anonymisation and that effective "anonymity" is rolled back with the advance of AI capabilities.

4 It will also discuss how obligations currently in the Personal Data Protection Act 2012[3] ("PDPA") could be applied to data protection concerns raised by AI development and applications.

5 The discussion will then address some possible directions that could be adopted in enhancing the PDPA's framework to complement and support ethical innovation.

6 In doing so, a case will be made that any governance model can develop in a consistent and evolutionary manner, and that it is possible to see further outlines and a pathway for developing a "light touch" legal framework that balances stakeholder interests.

II. Artificial intelligence and personal data

7 In matters of data protection under Singapore law and the PDPA, a threshold question to consider is whether or not a particular activity does, in fact, involve personal data. To begin with, definitions of "personal data" in the PDPA are technology neutral, focusing on the potential for identification of an individual (*ie*, "data, whether true or not, about an individual who *can* be identified").

8 Additionally, any discussion on anonymity must take into account nuances in the concept of the *capacity* for identification. One perspective is to consider the levels of *relative* anonymity and *degrees* of risk of re-identification in any situation (*eg*, hence the application of concepts such

3 Act 26 of 2012.

as "k-anonymity" or differential privacy[4]). Importantly, it should be noted that de-identification is not the same as anonymisation.

9 On this point, the PDPC's *Guide to Basic Data Anonymisation Techniques*[5] accepts that it is possible for "certain information" to be *inferred* from de-identified data and that "the problem of inference is not limited to a single attribute, but may also apply across attributes, even if all have had anonymisation techniques applied".[6] Where the capacity to infer the identity of an individual is present, the threshold question of whether "personal data" is involved is met.

10 One universally proclaimed promise of AI is the ability to infer information and extract insight[7] from data. With more and more data being recorded or made available,[8] the ability to infer identity or execute re-identification is a practical (and possibly unavoidable) state of affairs.[9] Indeed, it has been asserted that current anonymisation techniques are not a robust response to the proliferation (and availability) of data and the growing capacity of many technological solutions that can execute re-identification.[10]

---

4 Personal Data Protection Commission, *Guide to Basic Data Anonymisation Techniques* (25 January 2018) at para 16 and generally.

5 Personal Data Protection Commission, *Guide to Basic Data Anonymisation Techniques* (25 January 2018).

6 Personal Data Protection Commission, *Guide to Basic Data Anonymisation Techniques* (25 January 2018) at para 4.1(c).

7 For samples of analytics/artificial intelligence/machine learning use cases, see Robert Stanley, "Smart Implementation of Machine Learning and AI in Data Analysis: 50 Examples, Use Cases and Insights on Leveraging AI and ML in Data Analytics" *Engagement Optimization* (12 December 2017).

8 The growing ubiquity of Internet of Things applications, the proliferation and availability of data sources, *etc*, are all factors which contribute to the availability of information which can be used to identify an individual.

9 For an industry perspective, see Marty Graham, "AI Knows a Lot About 'Anonymous' Data Feeds—How Do We Find Out?" *Dell Technologies* (25 July 2018).

10 For a brief further discussion, see Yves-Alexandre de Montjoye *et al*, "Solving Artificial Intelligence's Privacy Problem" (2017) *Field Actions Science Reports* Special Issue 17, 80.

11 Even when one considers the use of technological countermeasures might be introduced to prevent or minimise re-identification,[11] one does have the sense that this resembles a classic arms' race between platforms and technologies that anonymise (in the name of good governance) and those that re-identify (in the name of delivering insight).

12 Additionally, it is often the case that data (including personal data) is used in the AI product development cycle (*eg*, from data preparation, the application of algorithms and the establishment of a model for a use case[12]).

13 Hence, though it will be a question of fact in each case, the ability to exclude the application of the PDPA in the development or use of AI applications by arguing that one has completely removed the capacity to identify a person will be limited, and grow increasingly so.

14 Where the PDPA is applicable, it is worth considering whether the current state of regulation it presents needs to be calibrated. Discussions about regulatory policy often measure regulation along a scale, with the abhorred fear of over-intrusive and burdensome potential regulations on the one end, and an irresponsible and excessively *laissez-faire* approach on the other end.

15 In this context, arguments for a "light touch" approach are usually grounded in the interests of not hindering of the growth of AI as a driver of economic growth and technological progress. This sentiment is neatly expressed in the UK House of Lords *Report of the Select Committee on Artificial Intelligence*:[13]

> Those arguing for a more cautious approach told us that poorly thought through regulation could have unintended consequences, including the

11 Measures include introducing "noise" into data sets to obfuscate the data or using Google's RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response <https://ai.google/research/pubs/pub42852> (accessed 16 April 2019).

12 For an overview of such a development and commercial cycle, see Personal Data Protection Commission, "Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI" (5 June 2018) at s 1(b) on "The AI Value Chain and Deployment Process".

13 United Kingdom, *Report of the Select Committee on Artificial Intelligence* (Report of Session 2017–19, 16 April 2018) at para 376 (Chairman: Lord Clement-Jones).

> stifling of development, innovation and competitiveness. Professor Love told us that there was a risk that 'AI specific regulation could reduce innovation and competitiveness for UK industry' as the competitive advantage gained by using artificial intelligence might be outweighed by regulatory burdens.

16 A similar sentiment was expressed by the UK Law Society in its submission to the Select Committee:[14]

> AI is still relatively in its infancy and it would be advisable to wait for its growth and development to better understand its forms, the possible consequences of its use, and whether there are any genuine regulatory gaps.

17 Indeed, there were witnesses in that report who were cited as expressing views that existing laws in the UK context may already "adequately cover AI".[15]

18 But there is a debate. The same report also cites alternative views. Some commentators argued not only for additional or new laws, but for new regulators. The discussion is more than a matter of legal analysis and clearly has political, economic and social dimensions which are well beyond the scope of this paper.

19 The PDPC itself has expressed a preliminary view in the PDPC AI Paper as to a preference for a "light touch" approach and has also elaborated on how this light-touch approach might take shape, by way of the Model Framework.

20 In this regard, it is worth noting the emphasis on self-governance in the Model Framework. It must be noted that one possible regulatory vision of AI includes notification or even registration requirements, which may include tagging or identification of AI elements used, coupled perhaps with controls on limits to the extent to which an AI product or service offering ("AI Offering") may be phased into an existing market for products or

14 United Kingdom, *Report of the Select Committee on Artificial Intelligence* (Report of Session 2017–19, 16 April 2018) at para 374 (Chairman: Lord Clement-Jones).

15 United Kingdom, *Report of the Select Committee on Artificial Intelligence* (Report of Session 2017–19, 16 April 2018) at para 374 (Chairman: Lord Clement-Jones).

services.[16] The Model Framework eschews this approach, and does not prescribe such an interventionist approach.

21 It is submitted that this is sound, given the current state of understanding and development both in the legal and technological spheres. Additionally, the full extent or ramifications of the potential for harm or good in AI Offerings is still unfolding and merits further study.

22 Indeed, it should be noted that data protection issues form only part of the wider range of potential issues that AI could raise,[17] and some issues (and their regulatory solutions) would be well beyond the scope of the PDPA. However, on the issue of data protection, the question is whether AI would introduce a wholly new (and hitherto unchecked or uncontemplated) issue or dimension to data protection matters that would require the current PDPA framework to undergo substantive legal reform.

III. Artificial intelligence and the Personal Data Protection Act

23 It is submitted that there are already lines of thought within the current PDPA framework which already provide some protection of the interests of data subjects in dealings with AI Offerings, and that new

16 A parallel, non-artificial intelligence example of this is in the realm of high-frequency trading algorithms, where foreign regulators (BaFin) have imposed designation (tagging) requirements for orders traded using algorithms, and imposed order-to-trade ratios to manage risks. See "Algorithmic trading and high-frequency trading" *BaFin* (updated 12 January 2018) <https://www.bafin.de/EN/Aufsicht/BoersenMaerkte/Hochfrequenzhandel/high_frequency_trading_node_en.html> (accessed 16 April 2019). The merits of such a regime in this case are context-specific, involving the management of organised markets, minimising flash crashes, *etc*.

17 In the European Group on Ethics in Science and New Technologies' "Statement on Artificial Intelligence and Robotics and 'Autonomous' Systems", data protection and privacy was only one of nine issues which included (a) human dignity; (b) autonomy (of the human being); (c) responsibility (for development and use of artificial intelligence ("AI")); (d) justice, equity, and solidarity; (e) democracy (ensuring human self-determination and wide enfranchisement in decisional processes in relation to AI); (f) rule of law and accountability; (g) security, safety, bodily and mental integrity; (h) sustainability; and (i) data protection and privacy.

legislation or regulatory developments should be incrementally added against this framework.

24 A survey of the current various obligations under the PDPA identifies key touchpoints that the Act may have in connection with the development or commercialisation of an AI Offering. Some of these are briefly covered below.

A. Consent, Notification, and Purpose Limitation Obligations[18]

25 The PDPA requires that organisations (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).

26 Earlier editions of this Digest have discussed the nuances of how such obligations might interact with data analytics use cases and their development.[19] For this article, it should be noted that a consent-centric regime, where the reasonableness of the consent asked for is limited (by the application of s 14(2)(*a*) of the PDPA[20]), can compel organisations to take pragmatic steps to build in appropriate opt-in and disclosure arrangements before they can secure lawful access to and use of personal data for developing and exploiting an AI Offering.

---

18 Personal Data Protection Act 2012 (Act 26 of 2012) Pt IV (Divisions 1 and 2).

19 See Lim Jeffrey, Sui Yin & Lee Yue Lin, "Data Analytics: Considerations When Repurposing Transactional Personal Data under the Personal Data Protection Act" [2017] PDP Digest 355.

20 The section requires that an organisation shall not "as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual". Leaving aside analytics for product/service improvement, use cases that go further (including, possibly, some forms of product/service R&D) may require an explicit and optional "opt-in" process, based on current rules. The reader is also invited to consider the discussion concerning the application of the so-called research exception as discussed in Lim Jeffrey, Sui Yin & Lee Yue Lin, "Data Analytics: Considerations When Repurposing Transactional Personal Data under the Personal Data Protection Act" [2017] PDP Digest 355.

27 Importantly, the Consent, Notification and Purpose Limitation Obligations (including the option to withdraw consent) do serve to place some level of governance obligations on the responsible development and commercialisation of AI Offerings, and provide data subjects with some degree of autonomy over the availability of their personal data for use.

28 In a similar vein, the Model Framework requires organisations to carefully consider giving data subjects the option to opt out of having their data used in AI Offerings. The Model Framework prompts organisations in this regard to take into account various factors.[21] Additionally, if organisations decide against giving the option to opt out, the Model Framework requires organisations to provide alternative recourses for reviewing their decision.[22]

B. Access and Openness Obligations[23]

29 The PDPC AI Paper proposes that decisions made by or with the assistance of AI should be explainable, transparent and fair.[24] Whilst "explainable" and "transparent" (as used in the paper) are not necessarily coterminous with the object or effect of the Access and Openness Obligations, those obligations do address the right of data subjects to be informed of how their personal data may have been used in an AI Offering, and establish a baseline obligation on an organisation to be able to explain how such personal data may have been used in respect of algorithmic decisions or machine learning applications.

30 The Model Framework has, in that vein, prescribed that organisations provide for "Customer Relationship Management" in dealing with matters

---

21 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at para 3.34.

22 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at para 3.36.

23 See s 21, and ss 11 and 12 of the Personal Data Protection Act 2012 (Act 26 of 2012), respectively.

24 Personal Data Protection Commission, "Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI" (5 June 2018) at p 5, s 2(i).

of transparency in the development and deployment of AI Offerings.[25] Transparency is also bolstered by the proposal that organisations develop a policy on what explanations to provide to individuals over how AI Offerings work in a decision-making process, how specific a decision was made, the reasons behind the decision, and the impact and consequences of the decision.[26] As the Model Framework hints, some of these measures are more than merely documentary in nature, such as the references in the Model Framework to Human-AI Interface design.[27]

31 Admittedly, there is still work ahead to address the balance between the need for clarity and transparency, and the need to preserve commercial, confidential and proprietary information and other aspects of the deployment of the AI Offering. Of particular concern is the issue of what would be a correct balance to be achieved, but the roots of a transparent approach akin to the Openness Obligations are there.

32 It is also conceded that there is a limit to how much of a correlation or equation can be made between transparency themes called for in discussions around AI, and the Access and Openness Obligations. For example, the Access Obligation has certain limitations (including those relating to revealing commercial information that could harm the competitive position of the organisation[28]), whilst the debates in AI regulation call for more robust disclosures. Indeed, the case for transparency in some of the literature concerning AI is predicated on safety justifications and on fostering trust in AI,[29] whereas the Access and Openness Obligations are focused on a more contained objective of providing a measured level of accountability in the collection, use and disclosure of personal data.

33 That said, it is possible to see how the Access and Openness Obligations could be augmented so as to apply to the same transparency

25 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at paras 3.27–3.36.

26 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at para 3.32.

27 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at para 3.33.

28 Personal Data Protection Act 2012 (Act 26 of 2012) Fifth Schedule, para 1(*g*).

29 For example, see United Kingdom, *Report of the Select Committee on Artificial Intelligence* (Report of Session 2017–19, 16 April 2018) at paras 95–106 (Chairman: Lord Clement-Jones).

interests discussed the context of AI.[30] Implicit in these existing obligations is a case for an AI developer to take steps to account for its use of personal data.

C. *Accuracy and Correction Obligations*[31]

34 Reported decisions in connection with the Accuracy Obligation are scarce,[32] and as worded, the statutory obligation appears to be a well-contained one. The obligation is to "make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete" where the personal data is "likely to be used by the organisation to make a decision that affects" the data subject, or "is likely to be disclosed" to another organisation.

35 Notably, the Accuracy Obligation focuses on the accuracy of the personal data, not the outcome. It therefore does not address all the broad *consequences* of decisions made on or disclosures made of accurate personal data (*eg*, issues of fairness, suitability, culpability of outcomes, *etc*).

36 For example, the personal data used in a data set may be factually accurate, but the AI Offering may produce skewed or inappropriate results if that personal data used reflects biased sampling. This may result in "inaccurate" outcomes, in a wider sense of failing to arrive at correct inferences.

37 Discussions on regulation of AI Offerings often go into debates about ensuring the quality, suitability and safety of the outcomes or use of the AI Offering. The aim of such regulatory themes is to apply governance frameworks that impose responsibility for the outcomes produced by the AI Offering, in some cases by targeting its design and development.

38 The Model Framework notably takes a facilitative approach, providing guidance as to what organisations may use as reference points to

---

30 Further detail and discussions could be considered over what data subject-facing statements could entail, and the extent to which an access obligation response related to incorporation or use of personal data in an AI Offering.

31 Sections 23 and 22 of the Personal Data Protection Act 2012 (Act 26 of 2012), respectively.

32 At the time of the writing of this article, the only reported example was *Re Credit Bureau (Singapore) Pte Ltd* [2019] PDP Digest 227.

strengthen the applicability and suitability of the AI Offering as exemplified in its proposals for repeatability assessments, counterfactual fairness testing, exception identification and handling,[33] traceability[34] and explainability.[35]

39 That said, there is a case to be made that accuracy (and applicability) of data determines the *quality* of an AI Offering. Real-life illustrations exist of the dangers of "AI gone bad" due to poor or bad data and, as one article profiled,[36] when discussing AI as deployed in a healthcare use case:

> If there are errors in the medical records, or in the training sets used to create predictive models, the consequences could potentially be fatal, a situation that sheds light on a key risk factor [in] AI implementations: the quality of your data practices.

40 A local illustration of this trend is in the similar fitness-for-purpose theme found in the Monetary Authority of Singapore's *Guidelines on Provision of Digital Advisory Services*.[37] Whilst the guidelines eschew express references to AI (for good reason), they prescribe a requirement on licensed digital advisers in developing client-facing solutions, to "ensure that the methodology of the algorithms behind the client-facing tool is sufficiently robust", collect all necessary information, conduct sufficient analysis, and perform sufficient testing "to detect error or bias" in algorithms.

41 In this light, it may be worth considering whether the Accuracy Obligation addresses more broadly the *quality* of personal data as applied in context[38] generally, and not mere factual congruence or completeness of

---

33 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at para 3.22.

34 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at paras 3.23 and 3.24.

35 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at para 3.17– 3.21.

36 Maria Korolov, "AI's biggest risk factor: Data gone wrong" *CIO* (13 February 2018). The reader is also referred to Danton S Char, Nigam H Shah & David Magnus, "Implementing Machine Learning in Health Care – Addressing Ethical Challenges" (2018) 378(11) N Engl J Med 981.

37 Monetary Authority of Singapore, *Guidelines on Provision of Digital Advisory Services* (CMG0G02, 8 October 2018) at para 31(a). See also "MAS Issues Guidelines to Facilitate Provision of Digital Advisory Services" (8 October 2018).

38 This includes a consideration of what would be relevant or applicable data.

personal data. If so, it may be possible to see a broad connection between the tasks of tackling the risk of bias or unsafe or harmful AI-based decision-making and the objectives achieved by compliance with the Accuracy Obligation.

42 Consistent with this perspective, the Model Framework guides organisations to build in a reactive quality control component so that organisations can address changes in situations or context, via regular model tuning,[39] and through active monitoring, review and tuning.[40]

43 In this vein, to the extent that the Correction Obligation compels the taking of steps to correct and alert recipients of errors in personal data, it can be said that the Correction Obligation represents or forms part of a legal remedial framework for addressing issues of improving the quality of personal data used or handled.

IV. Conclusion: evolutionary (versus revolutionary) development

44 This is not to argue that all aspects of data protection are already wholly settled and addressed under the current PDPA framework. Clearly, there are, even from the perspective of data protection issues only, issues to consider and further regulatory reform and work to be done. Principles adopted in the wider discussion on further issues raised on AI could well be fed back into the rules and regulations around the PDPA to enhance the current framework.

45 But this paper does suggest that the current framework of the PDPA can be adapted, using an evolutionary and incremental approach, to address data protection issues in respect of AI Offerings. Such an approach would indeed help practitioners, developers, consumers and other stakeholders work through issues in a way that is logical and follows a transparent and logically progressive path. This would be perhaps as important as aiming for a "light touch" approach.

---

39 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at para 3.25.

40 Personal Data Protection Commission, *A Proposed Model Artificial Intelligence Governance Framework* (January 2019) at para 3.26.

46 A "light touch" approach can mean different things to different audiences, but one perspective is that a regulatory approach is not "light touch" if it discourages use of AI Offerings because of fear, uncertainty and doubt in relation to their development and use. An important component of any "light touch" approach is therefore a gradual and logically progressive approach to addressing an issue – one which allows communities of practice to see a consistent and thread of development. Such an approach is more evolutionary than revolutionary, and the Model Framework interestingly aligns with this.

47 It is also submitted that "light touch" is not necessarily "self-governance", however tempting it may be for certain stakeholders to argue for such an approach. If self-governance means requiring organisations to "make their own way" or "make their own rules", questions can arise over whether such organisations are best placed or have the resources to do so. Consider, for example, whether it would have been more appropriate for the research exception to the Consent Obligation in the Third and Fourth Schedules of the PDPA[41] to leave questions of what constitutes the "public interest" to be determined as "what an organisation would determine as being in the public interest". One could argue that not all private enterprises are best placed or have the resources to make such potentially difficult and important evaluations.

48 In this regard, the Model Framework is a welcome step forward, as it provides an important frame of reference in addressing key issues and touchpoints for organisations to consider.

49 In keeping with the recognition of our evolving understanding of AI, a "light touch" approach may well favour open-ended, fact-based and weighted assessments so that there are no monolithic "one-size-fits-all" approaches to any issue. This would increase the importance of and reliance on providing well-crafted guidance, and invite community contributions to the issues to be discussed.

50 In closing, it is not the premise of this paper that the PDPA is a complete solution for all issues relating to AI.[42] Some issues are for wider

41 In particular, para 2(*d*) of the Third Schedule and para 4(*d*) of the Fourth Schedule.

42 For instance, one could identify scenarios where personal data may not be front and centre in the discussion – *eg*, road safety concerns in connection

(*continued on next page*)

forums[43] or other regulators (taking into account the relevant subject matter).[44] But, as Singapore considers its regulatory approach in this area, it is worth noting that that there is value in maintaining continuity and consistency and developing regulatory responses in a progressive and evolutionary manner.

---

with the functioning of autonomous vehicles: see the Road Traffic (Amendment) Act 2017 (Act 10 of 2017), read together with the Road Traffic (Autonomous Motor Vehicles) Rules 2017 (S 464/2017) (where the new ss 6C, 6D and 6E under cl 6 are relevant as they address the trials and uses of autonomous vehicles).

43 The breadth of issues is discussed in "Asilomar AI Principles" *Future of Life Institute* <https://futureoflife.org/ai-principles/?cn-reloaded=1> (accessed 1 May 2019). Examples of other issues include those raised in the context of artificial intelligence ("AI") as used in autonomous vehicles, where debates on ethical issues can occur (*eg*, the classic Trolley Problem). Other examples include the potential for AI to cause ethically questionable profiling by AI/algorithms (*eg*, the challenge by Mr Loomis against the prison sentencing decisions against him the Wisconsin Supreme Court).

44 For instance, in the field of financial technology, local examples of how accuracy and accountability are only part of the AI ethics/governance discussion can be found in the Monetary Authority of Singapore's FEAT Principles – see "Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector" (12 November 2018), which covers a wider canvas of issues.

BLOCKCHAIN RECORDS UNDER THE PERSONAL DATA PROTECTION ACT*

YEONG Zee Kin†
LLB (National University of Singapore),
LLM (Computer & Communications Law) (London);
Advocate and Solicitor (Singapore), Solicitor (England & Wales)

I. Introduction to blockchains

1 The current interest in blockchain technology can be attributed in large part to the immutability of blockchain records. While this is not an essay about how blockchains work, a brief description of how blocks of transactional records are created and chained provides a necessary introduction to its defining feature.

2 Briefly, the uniqueness of blockchain technology lies in how transactional records are organised into blocks and how blocks of records are linked in order to form the blockchain. Put simply, whenever a new block is created, the hash of its preceding block is incorporated as a data element in the new block. When a third block is created, the hash of the second block that is generated will include the hash value of the first block as one of the input data elements. It is therefore possible to picture how blocks are thereby linked together in a chain and imagine how each block contains ever decreasing traces of all preceding blocks.

3 One important feature of the hash is that it is a probabilistically unique signature that anyone reading the block with the correct cryptographic tool will be able to verify. If there is a change in the content of the preceding block, then its hash cannot be verified, thereby highlighting that records in the preceding block have been altered. Because

---

* An unabridged version of this article was first published in the *Singapore Law Gazette* (September 2018), available at <https://lawgazette.com.sg/feature/blockchain-records-under-singapore-law/> (accessed 20 February 2019).

† I wish to thank Albert Pichlmaier, Alex Toh and Yip Shue Heng for their comments on an earlier draft of this essay. All errors that remain are entirely mine. The views expressed in this essay are my personal views and should not be attributed to my employer.

each new hash will be created using the hash of the preceding block as one of its input, the effect of making changes to one block means that the hash values of all subsequent blocks have to be re-generated. This may be computationally feasible when dealing with a handful of records, but the older the record gets, the more computationally expensive this becomes.

4 The other important aspect of a blockchain is its distributed nature. Through a complex consensus algorithm, each new block is replicated to every node in the blockchain network. Not all participants in the network can add a new block. Currently, the most commonly known method of adding a new block is the proof of works method, popularised by Bitcoins. The first participant to complete a complex mathematical calculation is entitled to add a new block to the chain. As the number of mining nodes in the network increases, the number of participants working on mathematical problems increases. New blocks can be added to any of the mining nodes and once received, and verified, it will be replicated across the network of nodes.

5 While the proof of works method is common for public blockchains, this is computationally resource-intensive and slow. The alternative method that is currently gaining ground is proof of stake, which uses the percentage of stake that a miner has in the system to determine the probability that he can validate the addition of a new block: *eg*, if the participant has a 2% stake, then he has a 2% chance of validating a new block.[1] In private blockchains where participation is based on permission and there is a higher degree of trust amongst participants, neither proof of works or proof of stake is necessary.

A. Immutability of blockchain records

6 Combine the hashing function and the distributed nature of a blockchain network, and one can start to appreciate why it has been said that information in blockchains is *technically immutable*. This is a *theoretical claim* about how making changes to information in a blockchain is computationally infeasible, although not impossible. There lies the potential

1 "Proof of Work vs Proof of Stake: Basic Mining Guide" *Blockgeeks* <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/> (accessed 9 August 2018).

– to put into perspective, significantly unlikely – that sufficient participants in a public blockchain can collude to replace a past record in a block and recreate subsequent blocks. This is not a trivial task since a public blockchain can contain upwards of 10,000 nodes; but this becomes hypothetically possible when one considers the following two risks.

7 First, not all nodes on the network are mining nodes and it is the mining nodes that matter in a proof of work blockchain network. Second, controls of the mining nodes. The infrastructural and resource investment required for proof of works mining can discourage independent miners such that mining nodes are concentrated in the hands of serious players. The risk that some of these players acting in concert are able to marshal at least 51% of the compute power in the network becomes less remote.[2] Hence the game theory of the tragedy of commons, whereby even though there is a large number of nodes in a public blockchain, the number of active mining nodes can be sufficiently low that a 51% attack is possible.[3] Proof of stake blockchain networks address the risk of a 51% attack by limiting the number of trustworthy validators of new blocks in the network and determining each validator's chance of validating a new block based on his proportionate stake in the network.

8 But this is not to say that records in a public blockchain can never be altered. When the collective of participants in a public blockchain agrees to changes, it is possible that records be re-generated. There has been at least one notorious case (*ie*, Ethereum DAO) when the community agreed to fork the blockchain network – because they could not all agree to change past records – thereby creating two networks after a particular record.

9 Private (or permissioned) blockchains are limited to a smaller number of participants and are commonly used in commercial deployments of blockchain technology. The risk of unauthorised re-creation of past records arising from collusion increases (*ie*, 51% attack in a proof of work chain), although the likelihood, size and impact are still significantly ameliorated by reason of the distributed nature of the blockchain network. Moreover, the

2 See "Basic Primer: Blockchain Consensus Protocol" *Blockgeeks* at "#1 Proof of Work", <https://blockgeeks.com/guides/blockchain-consensus/> (accessed 11 August 2018).

3 See "Tragedy of the Commons" <https://en.bitcoin.it/wiki/Tragedy_of_the_Commons> (accessed 30 July 2018).

choice between using a public or creating a private chain is often driven by other considerations, for example whether the consortium is a closed one that requires members to agree to its club rules, the nature of the information that is transmitted and the transactions that are recorded, and whether the consortium members wish to keep these away from a more publicly accessible infrastructure.

B. Focusing on the ledger function of blockchain

10 While blockchain applications that are commonly featured in popular media have predominantly been in the area of cryptocurrencies and Initial Coin Offerings,[4] blockchain technology has gained traction as a building block in IT systems for commercial use in a number of areas. The range of proof-of-concepts and pilots that use blockchains have mushroomed in diverse areas like Know-Your-Customer,[5] trade finance,[6] supply chain management,[7] service-level agreements,[8] insurance,[9] and interbank

4 Technically, there is a difference between Initial Coin Offerings that create a new blockchain and those that create new cypto-tokens on an existing public blockchain (*eg*, Ethereum).

5 Priyankar Bhunia, "Consortium of banks, together with IMDA Singapore, completes proof-of-concept for ASEAN's first industry KYC Blockchain" *OpenGov* (28 October 2017).

6 Martin Arnold, "Banks team up with IBM in trade finance blockchain" *Financial Times* (5 October 2017); Elzio Barreto, "Hong Kong, Singapore to link up trade finance blockchain platforms" *Reuters* (25 October 2017); and Jamie Lee, "MAS to debut blockchain-based trade network with HK in 2019" *The Business Times* (15 November 2017).

7 Wolfie Zhao, "IBM Reveals Blockchain Supply Chain Trial with Singapore Port Operator" *coindesk* (16 August 2017); and "New blockchain based proof-of-concept to link digital trading platforms in Japan & Singapore" *Supply Chain Asia* (1 March 2017).

8 Giulio Prisco, "IBM and Bank of Tokyo-Mitsubishi UFJ Develop Blockchain-Powered Contract Management System" *BitCoin Magazine* (22 September 2016).

9 "AIG teams with IBM to use blockchain for 'smart' insurance policy" *TODAYonline* (15 June 2017).

settlements.[10] The focus of this essay is on blockchain as a building block of IT systems.

11 In particular, the focus of the legal analysis is the application of Singapore law on blockchain technology when it plays a record-keeping function. The record-keeping function of a blockchain can be analysed from the perspective that it is in essence a type of decentralised database. Indeed, it falls within the supergroup of distributed ledger technologies.[11] As a database, blockchains should raise no additional issues that our existing laws have not already addressed. However, the immutable nature of records stored in the blockchain network and the network's decentralised nature raise additional issues that do not usually surface when relational databases are used in a more traditional three-tier architecture for web-based application systems.[12]

12 Before we dive into a more involved legal discussion, we should fix the role and function of blockchain in context. In any commercial application, blockchain technology is deployed as one of its building blocks. Whether the blockchain that is utilised is a public or private one, it is probably not the only sub-system that performs an information-storing function. Invariably, a relational database is still necessary for the application system. The blockchain is used selectively, when the information that is stored on it or linked to it needs to be decentralised and to benefit from its technical immutability. For example, the details of a bill of lading may sit in a database while those data elements that are directly relevant for tracking its movement may be stored in the blockchain or linked to the chain. And these are only the components that deal with data storage and retrieval. In

10 Yasmine Yahya, "Singapore to launch blockchain project for interbank payments, among other fintech initiatives: MAS" (16 November 2016); and Stan Higgins, "Ubin Part 2: Singapore Central Bank Publishes Blockchain Project Details" *coindesk* (14 November 2017).

11 World Bank Group, "Distributed Ledger Technology (DLT) and Blockchain: FinTech Note No 1" (2017) <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> (accessed 22 May 2019).

12 *Ie*, a presentation tier, application tier and data tier: see "3-Tier Architecture: A Complete Overview" *JReport* and "Three-Tier Architecture" *techopedia* <https://www.techopedia.com/definition/24649/three-tier-architecture> (accessed 9 August 2018).

any application system, there are a number of other sub-systems involved, *eg*, communications, and programming logic implementing business rules.

II. Application of the Personal Data Protection Act 2012

13 The legal analysis in this section will concentrate on the Personal Data Protection Act 2012[13] ("PDPA") and the record-keeping aspects of the life cycle of personal data that is stored on or linked from blockchain networks. An unabridged version of this essay that was published in the *Singapore Law Gazette* (September 2018 issue) discussed various other areas of laws that have horizontal application, *eg*, proffering of blockchain records as primary evidence under the Evidence Act[14] and as original documents under the Electronic Transactions Act.[15]

A. Blockchain records containing personal data

14 Data protection laws are engaged whenever personal data is stored on or linked from the blockchain (the latter probably more common than the former) because of two reasons. First, it is the application system as a whole that will be considered when determining whether it processes personal data. Second, the definition of personal data is broad, looking at not only the dataset under consideration but also "other information to which the organisation has or is likely to have access".[16]

15 It is also useful at this juncture to remind the reader that the following discussion will also be relevant to information stored in the more traditional relational database sub-system of the application system that happens to also contain a sub-system that utilises blockchain. The discussion will focus on the maintenance and purging stages of the information life cycle.[17]

---

13 Act 26 of 2012.

14 Cap 97, 1997 Rev Ed.

15 Cap 88, 2011 Rev Ed. See Yeong Zee Kin, "Blockchain Records under Singapore Law" *Singapore Law Gazette* (September 2018).

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

17 See, for example, Malcolm Chisholm, "7 phases of a data life cycle" *Bloomberg Professional Services* (14 July 2015).

B. Maintaining and protecting personal data

16 During the maintenance stage in the information life cycle, the data controller has obligations to ensure accuracy and protection of the personal data. Ensuring the accuracy of information is an area which, if taken seriously, will involve significant investment of resources but can yield exponential benefits in terms of the insights that the organisation can derive and potentially the improvements to products and services that such insights may lead to for a business.

17 Information can be curated from multiple input channels, *eg*, updates from subsequent interactions with a customer, data cleansing as part of the organisation's data management programme, or upon request by the data subject to access and correct the personal data that the data controller holds. Under s 22 of the PDPA, it is not the case that every request by a data subject for correction must be automatously carried out. If "the organisation is satisfied on reasonable grounds that a correction should not be made",[18] it need not do so but "shall annotate the personal data … with the correction that was requested but not made".[19] Additionally, there are exceptions to the data subject's right to request for correction of his personal data, *eg*, opinions,[20] examination scripts and results, *etc*.[21]

18 Depending on the specific implementation and how it makes use of either a public or private chain, the information may be stored either in the block or the block may contain a pointer that references another location where the information is stored (and probably in a relational database). The correction of records could present some challenges that would require careful design and collaboration between computing engineers and legal advisers to address.

19 The blockchain record could itself be encrypted and signed, and its entire contents further hashed and inserted into the next block. The technical details of this chain effect and technical immutability have been discussed earlier. This makes changing information stored on a block,

---

18 Personal Data Protection Act 2012 (Act 26 of 2012) s 22(2).

19 Personal Data Protection Act 2012 (Act 26 of 2012) s 22(5).

20 Personal Data Protection Act 2012 (Act 26 of 2012) s 22(6) and s 1(*a*) of the Sixth Schedule.

21 See the Sixth Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012).

especially a confirmed block, computationally infeasible. One possible solution to giving effect to valid correction requests of personal data stored on the blockchain is to make use of annotations. This requires a bit of foresight during the design stage by incorporating data protection compliance considerations (*ie*, data protection by design): the application system can be designed to cater for a flag or other more detailed version marker that can be placed against a blockchain record. This flag can be used to determine (probably in conjunction with a separate version history table) whether that specific record is the accurate one from which personal data can be retrieved. Compliance with the correction obligation need not be a deletion of an older and inaccurate record, but it can be effected through treating such older and inaccurate records as obsolete while creating a new record that contains updated information.

20 The same solution may still be necessary even if the record is stored off-chain. The pointer to an off-chain relational database may contain a hash of that database record to ensure that changes to that record can also be detected. To preserve the integrity of the system, the same approach can also be taken when personal data stored in the relational database has to be corrected, *viz*, annotate that it is obsolete and point to a new record that is inserted into the database which contains the updated information. Thus, for this type of implementation, each correction will result in corresponding new blocks in the chain and a new record in the database.

21 The other important aspect during the maintenance stage is protection of personal data stored on the chain. This topic can be addressed briefly. If personal data is stored in the blockchain, the encryption of the block using Public Key Infrastructure will probably qualify as "reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks".[22]

22 However, it must be highlighted that the application programming logic plays an important role. It is through programming logic that the organisation controls whether these functions are limited to users who are authorised (or empowered to perform these functions) and the user access control or identity infrastructure performs the role of identifying and authenticating the user attempting to invoke these functions. The same observations are true where the blockchain contains a pointer that

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

references an off-chain relational database in which the personal data is stored. Thus, whilst one can have faith in the security and identity management capabilities of blockchain, one cannot be blind to the fact that blockchain is only one sub-system and that appropriate design considerations have to be taken holistically to ensure that the entire application system is reasonably secure.

C. Purging personal data from blockchain records

23 During the purging stage in the information life cycle, the data controller has to ensure proper disposal of the personal data. The purging could be a result of, for example, the data subject's withdrawal of consent and the personal data is expunged because there is no longer any purpose served in its retention; or it could be that the data has reached the end of its life cycle and the personal data is due for destruction in accordance with the organisation's destruction policy. Disposal of personal data can happen in a couple of ways: first, the anonymisation of the data such it is no longer possible to identify particular individuals while retaining sufficient granularity in individual records for future use; or second, through the deletion of the record. The challenge posed by blockchain records can be traced to the technical immutability: confirmed records are almost impossible to alter, much less delete. Even if the decision is to anonymise the records, this merely creates a new dataset without individually identifying information. The primary records are still in the chain. Thus, a solution is still required for deletion of the primary record.

24 One possible solution lies in the removal of "the means by which the personal data can be associated with particular individuals".[23] In other contexts, this would include anonymisation techniques. In the context of blockchain records, this could involve the disposal of the encryption keys such that it is now impossible to decrypt the information. This presupposes that the cryptography solution employs sufficiently strong encryption that brute force attempts to decrypt the cyphertext are computationally infeasible. This calls for a data protection by design approach at an early stage, selecting the right length of encryption key and encrypting all data elements that may potentially be personal data. Couple this with a well-documented process for destruction of the encryption key that can stand up

23 Personal Data Protection Act 2012 (Act 26 of 2012) s 25.

to scrutiny, and we may have a reasonable means of appropriately removing the association of each blockchain record to particular individuals.[24]

25 However, the effectiveness of this approach has to be assessed periodically since it is vulnerable to brute force decryption attempts. What is assessed to be computationally unfeasible today may no longer be the case when computation power benefits from quantum improvements, *eg*, when quantum computing becomes commercially accessible. That day is still a way off and perhaps, when that day arrives, there could be more durable solutions to this conundrum.[25]

D. Distributed nature of blockchain networks and transfer limitation

26 To round out the PDPA discussion, blockchain networks are also likely to face the same set of compliance issues as cloud services in relation to the limitation of transfers of personal data outside Singapore to countries that provide a comparable standard of protection. Blockchain networks, especially public ones, will have a multi-jurisdictional footprint.

27 The analysis of the issues must begin with the question of the role that the blockchain plays in the application system and what data is actually stored on the chain. The obligation to limit cross-border transfers to jurisdictions with comparable protection standards arises only if personal data is stored on the chain. If the data is stored in the relational database that is the main data sub-system, then this issue may not arise particularly when the database resides within jurisdiction. Should there be a need to transfer personal data, then the current set of solutions that deal with the use of cloud technologies can be applied with equal effect, *eg*, by contract, binding corporate rules or consent.[26]

28 It is not intended that we detour into a detailed discussion of how these mechanisms for ensuring comparable protection in the destination

---

24 See s 11(1) of the Personal Data Protection Act 2012 (Act 26 of 2012), which establishes the standard of reasonableness for compliance.

25 For example, Accenture has proposed the use of chameleon hashes as a way to allow future redaction of blockchain: Jeff John Roberts, "Why Accenture's Plan to 'Edit' the Blockchain is a Big Deal" *Fortune* (20 September 2016).

26 See regs 9 and 10 of the Personal Data Protection Regulations 2014 (S 362/2014).

jurisdiction operate. The function that the blockchain ledger is intended to perform will inform which of these mechanisms will be appropriate. For example, if the blockchain ledger is intended to track the transmission of purchase, delivery and shipping information of goods ordered through an e-commerce site, then the deemed consent may be sufficient as between seller and customer, while binding corporate rules are relied on for intra-group transfers and contractual clauses are relied upon for third-party logistics sub-contractors.

III. Conclusion

29 If there is one thing that the reader of this essay should depart with, it is the realisation that blockchain is but one of the building blocks of any application system or platform that makes use of distributed ledger technology. There does not appear that there are horizontal legal issues that cannot be solved by carefully planning for and incorporating data protection by design considerations early in the system architecture and design stage. Lawyers should also be aware that blockchain records are not the be all and end all of data storage sub-systems within an application system. Understanding its role and the data that is intended to be stored – and, equally important, how and in what form the data will be stored – will permit a more precise articulation of the issues and thence a set of bespoke contractual or other legal solutions to address them, within the context of the supporting legislative infrastructure that is currently available in Singapore. Thus, if there is one decision that the reader can make without remorse, it will be to decide to anchor the blockchain implementation in Singapore law.

DOES SINGAPORE HAVE A "RIGHT TO BE FORGOTTEN"?*

Nadia YEO†
LLB (Hons) (National University of Singapore),
Double Masters MPP–LLM (National University of Singapore);
Advocate and Solicitor (Singapore); CIPP/A

I. Introduction

1 Copying and sharing information have never been easier. All it takes is a click of a mouse button. Yet, once information is shared online, it can potentially last forever – what has been described as a problem of "digital eternity".[1]

2 The European General Data Protection Regulation ("GDPR") has extensive provisions allowing individuals to access, correct, block, and even erase their personal data. In particular, there has been considerable interest in the right to erasure in Art 17 of the GDPR, which has been analogised as a right to be forgotten following the decision of the Court of Justice of the European Union ("ECJ") in *Google Spain SL and Google Inc v Agencia Español de Protección de Datos (AEPD) and Mario Costeja González*[2] ("*Google Spain v Mario Costeja*").

3 This article provides an overview of the right to be forgotten and focuses on its current incarnation as the right to erasure in Art 17 of the

---

* Any views expressed in this article are the author's personal views and should not be taken to represent the views of her employer. All errors remain the author's own.

† Deputy Director (Legislation and Policy Advisory), Ministry of Home Affairs. Adjunct Law Lecturer, LASALLE College of the Arts. NUS WYWY Gold Medal Award recipient. She was previously an Assistant Chief Counsel at the Personal Data Protection Commission and is a member of the Law Society's Cybersecurity and Data Protection Committee. The author is indebted to the Personal Data Protection Commission and the Law Society's Cybersecurity and Data Protection Committee for the opportunity to contribute this article.

1 David Lindsay, "'The Right to be Forgotten' in European Data Protection Law" in *Emerging Challenges in Privacy Law: Comparative Perspectives* (Normann Witzleb *et al* eds) (Cambridge, 2014) at pp 290–293.

2 C-131/12 (13 May 2014).

GDPR. The article also studies the differences between the European Union's ("EU") right to be forgotten and the retention limitation obligation in the Personal Data Protection Act 2012[3] ("PDPA"), and offers views on the feasibility of implementing a right to be forgotten in Singapore.

II. The right to be forgotten

4 The concept of a right to be forgotten is frequently thought to have originated from the 13 May 2014 decision of the ECJ in *Google Spain v Mario Costeja*. However, it is actually not a new legal concept. While the decision of the ECJ certainly raised public awareness of the right, the obligation to delete personal data at the request of the individual once the data was no longer necessary preceded the decision. The principle underpinning the right to be forgotten was already contained in the EU Data Protection Directive ("EU Directive 95/46/EC"), on which the decision was premised) as early as 1995[4] and had been adopted by various EU member states in their national legislations.[5]

A. Facts in Google Spain v Mario Costeja

5 The facts in *Google Spain v Mario Costeja* are fairly simple. Mr Costeja had been declared insolvent in court proceedings that were reported in a Spanish regional newspaper in 1998. The articles naming Mr Costeja were made available online. Mr Costeja later discovered that any Internet user who typed his name in a Google search engine would be provided links to the articles regarding his insolvency and the confiscation order made at the

3 Act 26 of 2012.

4 Article 12 of the EU Directive 95/46/EC provided individuals a right of access to their personal data and required EU member states to guarantee every individual the right to obtain from the controller "… (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort".

5 Such as s 35 of the German Federal Data Protection Act (30 June 2017).

time against his property. This affected his ability to, among others, secure work.

6 He filed a claim with the Spanish data protection regulator AEPD against the Spanish newspaper, Google Spain, and Google Inc. In his claim, he sought orders for the newspaper to erase his name from the articles and for his personal data to be removed from the search results provided by Google to Internet users. He argued that the facts in the article no longer reflected reality and that any reference to the insolvency proceedings and confiscation order in the articles were hence irrelevant.

7 AEPD dismissed the claim against the newspaper on the basis that the articles had been lawfully published online on the date they were issued. However, it upheld the claim against Google Spain and Google Inc on the basis that search engines were personal data processors and therefore had to erase the personal data returned in the search results they generated when the personal data was no longer required. AEPD based its decision on the presence of a requirement, found in the EU Directive 95/46/EC, for personal data to be deleted when no longer required.

8 Google Spain and Google Inc appealed against the decision to the High Court of Spain, which referred a series of questions to the ECJ on the correct interpretation and application of EU law,[6] in particular EU Directive 95/46/EC. In short, the ECJ was asked whether an individual has the right to request that his or her personal data be removed from accessibility via a search engine (the "right to be forgotten").

9 The ECJ found that on the facts of the case, the interference with a person's right to data protection could not be justified by the economic interests of the search engine. Google was obliged to remove from its search results any links to webpages hosting the information sought to be suppressed if processing the personal data contained in the information was incompatible with the EU directive.

6 This includes Arts 7 and 8 of the Charter of Fundamental Rights of the European Union.

10 In fact the ECJ's decision in *Google Spain v Mario Costeja*[7] was premised on its interpretation of the EU Directive 95/46/EC and its application to search engines.

11 The ECJ had observed that the directive provided individuals with a right – under certain conditions – to request search engines to remove links containing personal data about them. This right applied when the personal data published online was inaccurate, inadequate, irrelevant, or excessive for the purposes of the data processing.[8]

12 At the same time, the ECJ expressly clarified that the right to be forgotten was not absolute but needed to be balanced against other fundamental rights such as the freedom of expression and of the media.[9]

13 The case itself provided an illustration of how the right to be forgotten had to be balanced with other considerations. Although the ECJ ordered Google to delete access to personal data deemed irrelevant by the complainant, it also emphasised that the content of the underlying newspaper archive should not be changed in the name of privacy.[10] It was enough, for the purposes of preserving an individual's privacy, that his personal data was still accessible but no longer ubiquitous online.

---

7 The Court of Justice of the European Union also held that (a) the activity of an Internet search engine provider should be considered "data processing", as defined in Directive 95/46/EC ("the Directive") of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with respect to the processing of their personal data and the free movement of such data (the Directive); (b) Internet search engine providers should be considered "data controllers", as defined in the Directive, as they decide on the purposes and means of processing the data; and (c) the data protection regulations of an EU member state should apply to subsidiaries that are performing data processing activities in the state even if its parent company is not established there.

8 *Google Spain SL and Google Inc v Agencia Español de Protección de Datos (AEPD) and Mario Costeja González* ("*Google Spain v Mario Costeja*") C-131/12 (13 May 2014) at [93].

9 *Google Spain v Mario Costeja* C-131/12 (13 May 2014) at [85].

10 *Google Spain v Mario Costeja* C-131/12 (13 May 2014) at [88].

B. Effect of the Court of Justice of the European Union's decision

14 The scope of application of the right to be forgotten in the ECJ's decision continues to be contested by Google to this day.[11] Google maintains a list of requests it obtains for removal of search results in its published Transparency Report.[12] As of 7 May 2019, it had received 801,322 requests to delist or remove personal data on 3,122,565 URLs. Of these requests, Google acceded to the deletion of approximately 44.5 per cent of requests.

15 Yahoo! and Microsoft's Bing also began processing requests for deletion of personal data in their respective search engine results in July 2014 following the decision of the ECJ.[13] As at June 2018, Bing received 26,729 requests relating to 78,781 URLs,[14] and acceded to the deletion of approximately 42 per cent of requests.

16 Other organisations have also been circumspect about implementing the right to be forgotten and are slow to provide the means for individuals to easily delete their personal data. Their reluctance to embrace this right is perhaps understandable. In practice, the selective deletion of a particular individual's personal data often presents companies with considerable technical, organisational, and sometimes even legal challenges.

17 However, despite the challenges that may arise in the implementation of the right to be forgotten, it is clear that this right is here to stay in its latest incarnation as Art 17 of the GDPR.

---

11 Google is currently locked in dispute with France's data protection agency Commission Nationale de l'Informatique et des Libertés, which is arguing that the right to be forgotten should apply to the search engine's results globally and not just within the European Union. Advocate General Maciej Szpunar issued an opinion in January 2019 advising that Google can limit the "right to be forgotten" to Internet searches made in the European Union.

12 Google, "Search Removals Under European Privacy Law: Google Transparency Report" (7 May 2019) <http://www.google.com/transparency report/removals/europeprivacy/?hl=en> (accessed 7 May 2019).

13 Lisa Fleisher, 'In Europe, Microsoft and Yahoo Have Started to Forget" *The Wall Street Journal* (28 November 2014).

14 Bing, "Request to Block Bing Search Results in Europe" (2015) <https://www.bing.com/webmaster/tools/eu-privacy-request>; "Bing, Content Removal Requests Report" *Microsoft* (2018) <https://www.microsoft.com/en-us/corporate-responsibility/crrr> (accessed 20 April 2019).

III. General Data Protection Regulation and the right to erasure

18 The GDPR came into effect on 25 May 2018. Unlike the EU Directive 95/46/EC, the GDPR requires no further transposition into EU member states' local laws and is enforceable as is on all EU member states. The GDPR grants several rights to individuals; this includes in Art 17 of the GDPR a right for individuals to have their personal data erased.

19 The right to erasure in Art 17 of the GDPR has been analogised as a "right to be forgotten" as it gives rise to an obligation to delete personal data belonging to individuals upon request. However, unlike a right to be forgotten, the right to erasure is not an unfettered right. It may be exercised only on the basis of the following grounds, namely:

(a) where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
(b) where previously given consent to process the personal data has been withdrawn and there is no other legal processing basis to continue retaining the personal data;
(c) where the right to object to data processing is exercised (in general and in the context of direct marketing) and there are no other overriding legitimate grounds to continue processing the personal data;
(d) where the personal data has been processed in an unlawful way;
(e) where the personal data has to be erased for compliance with a legal obligation in the EU or member state laws to which the data controller is subjected to; and
(f) where the personal data relates to children and has been collected via information society services.

20 Further, the right to erasure would not apply where data processing is necessary for any of the following reasons:

(a) exercising the right of freedom of expression and information;
(b) compliance with a legal obligation which requires processing by the EU or member state laws to which the data controller is subject, or for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the data controller;
(c) public interest in the area of public health;

(d) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the exercise of the right to erasure would render impossible or seriously impair the achievement of the objectives of this processing; or

(e) the establishment, exercise or defence of legal claims.

21 Article 17 does not only apply to organisations established in the EU. Article 3 of the GDPR extends the reach of the obligations in the GDPR to organisations that may be established outside the EU if they are targeting EU individuals. Organisations based in Singapore may have to abide by the requirements in Art 17 if they process personal data of individuals in the EU if they offer goods and services to EU individuals or monitor the activities of individuals in the EU. We can immediately surmise that organisations with an online presence (which websites would typically include some web tracking functionality via cookies or social plug-ins) would be affected by these requirements and have to work on establishing processes to comply with the right to erasure in Art 17.

22 Administrative penalties under the GDPR can go up to €20m or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The high penalties that may be imposed under the GDPR ensure that any cost-benefit analysis undertaken by organisations in weighing the compliance costs and risks would be in favour of adherence to the requirements to allow individuals the exercise of their right to be forgotten.

IV. Retention limitation obligation in Singapore

23 Any notion of a right to be forgotten in Singapore may stem from the presence of the retention limitation obligation in the PDPA. However, the retention limitation obligation in the PDPA is quite unlike a right to be forgotten. The Personal Data Protection Commission ("PDPC") in fact clarified in a *Straits Times* Forum reply dated 12 June 2014[15] that the PDPA does not provide for a right to be forgotten.

---

15 Evelyn Goh, "Protection of Personal Data Important" *The Straits Times Interactive Online* Forum reply (12 June 2014). The response by the Personal Data Protection Commission was made shortly in the aftermath of the decision of the Court of Justice of the European Union in *Google Spain v*

(*continued on next page*)

24 Similar to the implementation of the right to be forgotten in *Google Spain v Mario Costeja*, and its subsequent enactment as the right to erasure in Art 17 of the GDPR, the enactment of the retention limitation obligation in Singapore involves a balancing of competing interests. However, unlike the EU, which recognises privacy as a fundamental right for EU individuals,[16] Singapore had enacted the PDPA as a baseline law to protect individuals' personal data.[17]

25 The retention limitation obligation in the PDPA is certainly limited compared to Art 17 of the GDPR and, it appears, correctly so in order to balance the twin objectives of the PDPA – namely "individuals' interests" versus "the need to keep compliance costs manageable for organisations".[18] The approach is a pragmatic one as the legislation neither promises uncurtailed protection of an individual's informational privacy nor creates trade barriers.[19]

26 Under the PDPA, organisations are obliged not to retain the personal data of individuals or to remove the means by which the personal data can be associated with particular individuals if they no longer require the data (a) for the purposes for which the data was collected, and if (b) there are no business or legal reasons to continue retaining it. The decision of the PDPC in *Re Social Metric Pte Ltd*[20] confirmed that the two limbs (a) and (b) of the retention limitation obligation in the PDPA were meant to be read conjunctively. This means that an organisation need only establish that it has purposes for retaining an individual's personal data under *either* limb in order to be allowed to continue retaining the data. The retention limitation obligation hence provides organisations with a wider set of reasons to justify their continued retention of individuals' personal data compared to the requirements of Art 17 of the GDPR.

Mario Costeja C-131/12 (13 May 2014), which was seen as an affirmation of the application of the right to be forgotten in EU member states.

16 Charter of Fundamental Rights of the European Union Art 8.

17 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(6).

18 *Parliamentary Debates, Official Report* (15 October 2012), vol 89 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

19 Yip Man, "Personal Data Protection Act 2012: Understanding the Consent Obligation" [2017] PDP Digest 266.

20 [2018] PDP Digest 281.

27 Although the PDPA does not prescribe the duration for which organisations may retain individuals' personal data, organisations would have to comply with any legal or specific industry-standard requirements that may apply in relation to the retention of data.[21] The decision of the PDPC in *Re Credit Bureau (Singapore) Pte Ltd*[22] ("*Credit Bureau*") is apposite. In that case, the organisation (a financial institution) had displayed bankruptcy-related information, including "HX" ratings, about the complainant for five years in its Enhanced Consumer Credit Report. Although the complainant argued that the information published was no longer relevant and that the purpose for which the organisation had collected the information was no longer required, the PDPC found that the duration of five years was aligned with the display period of publicly available insolvency search results maintained by the Insolvency and Public Trustee Office (of Singapore).[23] The PDPC took the view that a five-year personal data retention policy would provide financial institutions with a useful credit history of potential borrowers to facilitate their lending decisions and that the organisation's continued retention (and publication) of the complainant's bankruptcy-related information was justified as a valid business purpose.[24] This is quite unlike Art 17 of the GDPR, which may require the immediate deletion of personal data if continued retention is objected to or previously provided consent to retain the personal data has been withdrawn.

28 The PDPC's decision in *Credit Bureau* also illustrates clearly the differences between the retention limitation obligation in the PDPA and the right to be forgotten in *Google Spain v Mario Costeja*. Although the two cases had similar fact situations,[25] they had very different outcomes in the two jurisdictions applying their respective data protection laws.

---

21 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 18.4.

22 [2019] PDP Digest 227.

23 *Re Credit Bureau (Singapore) Pte Ltd* [2019] PDP Digest 227 at [9].

24 *Re Credit Bureau (Singapore) Pte Ltd* [2019] PDP Digest 227 at [10].

25 Although both *Re Credit Bureau (Singapore) Pte Ltd* [2019] PDP Digest 227 and *Google Spain v Mario Costeja* C-131/12 (13 May 2014) relate to information concerning the bankruptcy of the respective complainants, and the arguments raised by the complainants were similar, the application of the

(*continued on next page*)

29 It goes without saying that the retention obligation does not go so far as to provide individuals with the ability to have their personal data deleted upon request. Under the PDPA, organisations need not interface with individuals when deciding whether or not to continue keeping or to delete their personal data. While the retention obligation certainly facilitates organisations' control over the personal data they have collected and may be said to provide them with greater autonomy over their business decisions, it does not add to individuals' autonomy and control over their personal data.

V. Should the right to be forgotten be imported to Singapore?

30 In its reply to *The Straits Times* Forum article in 2014, the PDPC had observed that the right to be forgotten was yet to be adopted by many jurisdictions and that it was monitoring developments on the issue.

31 In September 2016, Access Now, an international organisation that defends and extends the digital rights of users at risk around the world, conducted a study of the right to be forgotten and its adoption, if any, in the legislations of various jurisdictions around the world.[26] At the time, it found that most countries had only just begun to engage in conversations regarding the right to be forgotten and that countries that took steps to introduce the right did so only in limited forms.[27]

32 However, given that the GDPR has now embraced the right to be forgotten, it would be interesting to observe whether the PDPC would be willing to follow suit in the years to come.

---

different obligations under the EU Directive 95/46/EC and the Personal Data Protection Act 2012 (Act 26 of 2012) resulted in very different outcomes.

26 Access Now, "Position Paper: Understanding the 'Right to be Forgotten' Globally" (September 2016).

27 For example. in South Korea, the Korea Communications Commission, a government agency, developed guidelines aimed at providing a right to be forgotten in the country. However, its version of the right was limited and varied significantly from the right that had developed in the European Union. First, the right was not established in law. Second, it primarily concerned online users' own posts rather than articles posted by third parties since Korean law already grants individuals a right to request the deletion of information by a third party if the information resulted in reputational loss. Third, the guidelines limited the exercise of the right to "exceptional cases".

33 Compliance with the requirements of Art 17 of the GDPR will mean that there will be a growing number of organisations around the world, particularly those with data processing activities in the EU, that would have enacted processes or workflows to allow compliance with the requirements to delete personal data about individuals on request.

34 Increasingly, the issue of compliance costs in providing individuals with a right to be forgotten will become less pertinent in the equation of arguments for and against providing such a right and in striking that appropriate balance in the PDPA.

ENABLING CROSS-BORDER DATA TRANSFERS IN A GLOBAL ECONOMY*

LIM Chong Kin†
LLB (Hons) (National University of Singapore),
LLM (National University of Singapore);
Advocate and Solicitor (Singapore), Solicitor (England and Wales)

Janice LEE‡
LLB (Hons) Law with Chinese Law (University of Nottingham);
Advocate and Solicitor (Singapore); CIPP/E

I. Introduction

1 Much has been said about the importance of allowing data to be transferred across borders freely, both within ASEAN as well as globally, so as to maximise the potential in the digital economy.

2 It is undeniable that data is the lifeblood of the digital economy and international trade. In the past decade, international data flows have increased the global GDP by 10.1 per cent in what has been termed the "digital globalisation".[1] In 2014, data flows accounted for US$2.8trn of the

---

* 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* and *Chambers Asia Pacific: Band 1 for TMT*. He has also 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*.

‡ Associate Director, Telecoms, Media & Technology Practice Group, Drew & Napier LLC. Janice is a Certified Information Privacy Professional (Europe) (CIPP/E).

1 James Manyika *et al*, "Digital Globalization: The New Era of Global Flows" *McKinsey Global Institute* (March 2016) at p 76.

global GDP, a larger share than the global trade in goods, and Asia Pacific surpassed North America as the world's largest e-commerce market with US$525.5bn in business-to-consumer e-commerce sales.[2] Cross-border flow of data has helped small- and medium-sized enterprises reach global markets by joining e-commerce marketplaces with consumers expected to spend US$1trn on e-commerce by 2020.[3]

3 Cross-border data flows are also exploding in volume, having grown 80 times larger between 2005 and 2016.[4] Apart from data flows generated by individuals through e-mails, e-commerce transactions and social media posts to name a few, trade and production in today's global information economy are heavily dependent on moving, storing and using data across borders. Multinational corporations and, increasingly, organisations of all sizes across all sectors rely heavily on cross-border data flows to coordinate and monitor international production systems, manage global workforces, and support products in the field in real time.

4 The rapid adoption of emerging technologies such as cloud computing, data analytics, the Internet of Things (or IoT) and artificial intelligence, which depend on the movement and processing of data, has further increased the importance of data as an input to commerce, affecting not just information industries but also traditional industries.[5] Furthermore, international e-commerce transactions cannot take place without collecting and sending personal data such as customers' names, addresses and billing information.

5 As businesses are increasingly using the personal data of individuals to gain business and behavioural insights to provide better products and services to customers, there is a corresponding need to ensure that personal data is used responsibly and is adequately protected from abuse or

2 GSMA, "Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC Can Protect Data and Drive Innovation" (September 2018) at p 10.

3 James Manyika *et al*, "Digital Globalization: The New Era of Global Flows" *McKinsey Global Institute* (March 2016) at p 45.

4 Susan Lund & James Manyika, "Defending digital globalization" *McKinsey Global Institute* (20 April 2017).

5 Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" *Information Technology and Innovation Foundation* (1 May 2017) at p 6.

unauthorised access or disclosure across the entire processing lifecycle, regardless of where it is processed.[6]

II. Restrictions on cross-border data transfers

6 At present, however, the global landscape for cross-border data transfers appears quite discordant. Data protection laws, where they exist, vary by jurisdiction, as different countries have differing views on what is the appropriate amount of protection for personal data. While these instruments and laws share some common principles, "they do not create an interoperable regulatory framework that reflects the realities, challenges and potential of a globally connected world".[7]

7 Some countries do not impose material restrictions on cross-border transfers of personal data but require organisations, by legislation or jurisprudence, "to remain 'accountable' for the continued protection of transferred data at the level it is protected inside the jurisdiction".[8] The US in particular has taken an approach that is focused on accountability. There is generally no restriction on the movement of data out of the US but organisations are accountable for any use of the data by the organisations or their suppliers. The accountability approach has permitted their national digital goods and services businesses to grow rapidly, and arguably, dominate much of the international economy in digital goods and services.[9]

8 In contrast, the European Union ("EU") has adopted the General Data Protection Regulation ("GDPR"), which is intended to provide consistent EU-wide protection of personal data and for the transfer of

---

6 GSMA, "Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC Can Protect Data and Drive Innovation" (September 2018) at p 12.

7 GSMA, "Safety, Privacy and Security Across the Mobile Ecosystem: Key Issues and Policy Implications" (2017) at p 37.

8 For example, the US, Canada and Mexico. Center for Information Policy Leadership, "Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy" (25 September 2017) at p 1 <https://www.informationpolicycentre.com/enabling-global-data-flows.html> (accessed 4 March 2019).

9 GSMA, "Cross-Border Data Flows: Realising Benefits and Removing Barriers" (September 2018) at p 14.

personal data within the EU and to third countries which are deemed to have "adequate" data protection regimes. Under the GDPR, organisations which demonstrate to data protection authorities that they can handle personal data responsibly, either through "binding corporate rules" or certifications, can benefit from general permissions to transfer personal data out of the EU.

9 Many countries have adopted variations of a model based on the EU data protection laws. Countries prohibit cross-border transfers of data if the receiving country's laws are not substantially similar to their own and thus deemed not "adequate", unless certain specified derogations apply, or the transfers can occur under an exempted mechanism or recognised alternative transfer structure. These include concepts such as "standard contractual clauses, binding corporate rules, cross-border privacy rules or bi- or multilateral cross-border transfer arrangements".[10]

10 The Singapore Personal Data Protection Act 2012[11] ("PDPA") imposes restrictions on the transfer of personal data to other countries that do not have similar data protection laws or standards. Under s 26 of the PDPA, all transfers of personal data outside Singapore are prohibited unless one of the exceptions applies (the "Transfer Limitation Obligation"). An organisation shall not transfer any personal data to a country or territory outside Singapore, except in accordance with requirements prescribed under the PDPA to ensure that the organisation provides a standard of protection to the personal data transferred that is comparable to the protection under the PDPA. The Personal Data Protection Regulations 2014[12] in turn set out the detailed requirements which organisations are required to comply with in order to ensure a comparable standard of protection.

11 The Transfer Limitation Obligation falls on the organisation sending the personal data overseas, *ie*, the transferring organisation, to take appropriate steps to ensure that it will comply with its data protection obligations under the PDPA in respect of the personal data transferred

10 Center for Information Policy Leadership, "Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy" (25 September 2017) at p 2 <https://www.informationpolicycentre.com/enabling-global-data-flows.html> (accessed 4 March 2019).

11 Act 26 of 2012.

12 S 363/2014.

while it remains in its possession or under its control.[13] The transferring organisation is also required to take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data outside Singapore is bound by legally enforceable obligations to provide the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

12 While the PDPA imposes restrictions on the transfer of personal data outside Singapore, businesses are given the flexibility to craft contractual provisions that meet their business and data-handling needs for the purposes of cross-border transfer of data. Under reg 10 of the Personal Data Protection Regulations, legally enforceable obligations include obligations imposed on a recipient of personal data under, among other things, any law, contracts requiring the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA, binding corporate rules or other legally binding instruments. Unlike the GDPR, the PDPA does not require parties to use non-modifiable standard contractual clauses or to obtain the data protection authority's prior approval of such cross-border transfer of data contracts.

A. Data localisation requirements

13 A number of countries have also introduced data localisation requirements which restrict the cross-border flow of data by requiring companies to store data on servers located within their borders. These requirements may cover most or all types or data, or only specific types of data, such as requiring payments to be processed locally or personal information such as medical records or tax records to be stored within the country.

14 Although there are many motivations behind the restrictions on data flows, advocates typically argue that such restrictions protect data from surveillance by foreign governments and enable the government to maintain access to the data stored on its territory. Some policymakers also believe that data localisation requirements will create local technology jobs. It is generally agreed, however, that data localisation policies present a new

13 Personal Data Protection Regulations 2014 (S 363/2014) reg 9.

barrier to digital trade as it makes cross-border data flows harder and/or more expensive and puts foreign firms at a disadvantage.[14] Data localisation requirements typically also increase the cost of doing business because they force Internet companies and online platforms to build duplicate server locations in order to meet localisation requirements.[15]

III. The case for international interoperability in data protection

15 Cross-border data transfers are currently regulated by a patchwork of international, regional and national instruments and laws. In the same way, personal data is regulated by a variety of geographically-bound privacy regulations with varying standards of personal data protection.

16 As businesses that are bound by these laws often operate regionally or internationally, the lack of harmonisation of data protection regulations makes it costly and time-consuming for them to navigate the ambiguity of the differing regulations and requirements. While businesses want to be able to roll out their latest cutting-edge digital service or data-driven innovation, they often face the challenge of having to grapple with a complex regulatory web of differing requirements across the region and internationally before they are able to take their product to market.

17 In particular, medium-large enterprises that have operations across multiple countries, but do not have the legal resources of multinational corporations, are likely to be the hardest hit by compliance costs as they may not have the resources to deal with the restrictions in all the countries in which they may have customers.

18 As the global economy shifts further into a borderless, interconnected environment, it is essential to strike the right balance between the need to ensure that there are safeguards to protect and secure personal data wherever it goes, and the benefits from the seamless and free flow of data. Creating interoperable data protection rules or an international regulatory or legal framework will ensure greater legal certainty and predictability, reduce

14 Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" *Information Technology and Innovation Foundation* (1 May 2017) at pp 6-7.

15 Susan Lund & James Manyika, "Defending digital globalization" *McKinsey Global Institute* (20 April 2017).

barriers to trade and investment and create a clearer compliance environment for businesses that wish to operate in the country.

19 Regional privacy frameworks play an important role in driving towards a common high standard of personal data protection that will contribute to the promotion and growth of regional and global trade and flow of data. They drive further alignment of data privacy laws and co-operation between enforcement authorities not just within a region, but also between regions.[16]

20 In this vein, two main privacy frameworks, namely the ASEAN Framework on Personal Data Protection ("ASEAN Data Protection Framework") and the APEC Privacy Framework and its accompanying systems, have been developed and implemented to encourage convergence across the region to allow the free flow of data while ensuring that there is a similar level of protection accorded to personal data.[17]

A. ASEAN Data Protection and Digital Data Governance Frameworks

21 In recognition of the importance of fostering regional integration and co-operation to strengthen personal data protection and ensure the free flow of data across the region, the ASEAN Telecommunications and Information Technology Ministers Meeting ("TELMIN") adopted the ASEAN Data Protection Framework in November 2016. Its objective is to strengthen the protection of data in ASEAN and to facilitate co-operation among the participating member states with a view to contributing to the promotion and growth of regional and global trade and information flows.[18]

22 The ASEAN Data Protection Framework recognises two broad avenues through which transfer of personal data are permitted, namely

16 GSMA, "Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC Can Protect Data and Drive Innovation" (September 2018) at p 11.

17 GSMA, "Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC Can Protect Data and Drive Innovation" (September 2018) at p 11.

18 ASEAN Framework on Personal Data Protection (25 November 2016) at para 1 <https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> (accessed 4 March 2019).

(a) a consent-based approach, where the consent of the individual has been obtained for the transfer, and (b) an approach to ensure consistency with the seven principles of the ASEAN Data Protection Framework, where the organisation transferring the data takes steps to ensure that the recipient will protect the personal data consistently with the principles.

23 The ASEAN Data Protection Framework does not create any legally binding domestic or international obligations. ASEAN member states implementing the ASEAN Framework at a domestic level are also free to adopt exceptions that suit their particular domestic circumstances.[19]

24 More recently, the ASEAN TELMIN endorsed the ASEAN Framework on Digital Data Governance ("ASEAN Digital Data Governance Framework") which is aimed at "strengthening the data ecosystem, achieving legal and regulatory alignment of data regulations and governance frameworks, and fostering data-driven innovation across ASEAN member states to boost the growth of digital economy in the region".[20] One of the initiatives under the ASEAN Digital Data Governance Framework is a cross-border data flow mechanism within ASEAN to facilitate data flows between participating ASEAN member states, although the framework notes that the specifics of the mechanism will need to be worked out.

25 While these are certainly positive developments, the road to harmonisation is likely still a way off given the different stages of maturity in terms of data privacy laws (or lack thereof) in the ASEAN member states, as well as the costs of implementation, skills and expertise required to manage the harmonisation process.

---

19 For example, Vietnam recently passed a new cybersecurity law permitting its government to collect e-data related to acts in cyberspace infringing, among others, national security and social order. This would appear to fall within the exception for national sovereignty, national security, public safety, public policy, and governmental activities, contained in para 4(b) of the ASEAN Data Protection Framework. This permissive approach under the ASEAN Data Protection Framework, allowing the member states to choose the extent of application of its principles, is generally consonant with ASEAN's consensus rather than prescriptive approach to matters.

20 Joint media statement on the ASEAN Digital Data Governance Framework (6 December 2018) at para 4 <https://asean.org/storage/2018/12/TELMIN-18-JMS_adopted.pdf> (accessed 4 March 2019).

B. APEC Cross-Border Privacy Rules

26 The APEC Privacy Framework consists of nine guiding principles to help APEC member economies develop a consistent domestic approach to the protection of personal information. The APEC Privacy Framework forms the basis for the APEC Cross-Border Privacy Rules ("CBPR"), a voluntary certification scheme that seeks to ensure the continued free flow of personal information across borders across APEC economies taking part in the initiative while establishing a voluntary accountability mechanism for meaningful protection of the privacy and security of personal information.[21]

27 There are three major elements of APEC CBPR:[22]

(a) adoption of shared principles in the treatment of personal data;
(b) creation of enforcement mechanisms where data is transferred between member economies; and
(c) accountability of organisations that must be able to demonstrate that they have certain safeguards in place before they are granted a general permission to transfer data.

28 The Privacy Recognition for Processors ("PRP") employs a similar accountability system to CBPR for data processors.[23] The Cross-Border Privacy Enforcement Arrangement is a multilateral mechanism that encourages co-ordination among data privacy authorities.

29 As the APEC region is very diverse, the CBPR is designed to be a very pragmatic instrument, which reflects the institutional characteristics of APEC as a non-binding organisation that encourages economic growth

---

21 Maria Vasquez Callo-Muller, "GDPR and CBPR: Reconciling Personal Data Protection and Trade" *Asia-Pacific Economic Cooperation* (October 2018) at p 3. There are currently eight participating economies, namely, the US, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia and Chinese Taipei.

22 GSMA, "Cross-Border Data Flows: Realising Benefits and Removing Barriers" (September 2018) at p 15.

23 As the APEC Cross-Border Privacy Rules only apply to controllers of personal information, the Privacy Recognition for Processors system is a certification mechanism for data processors to demonstrate their ability to provide effective implementation of a personal information controller's privacy obligations related to the processing of personal information.

based on facilitated trade and investment.[24] It establishes bottom line standards for personal data protection to facilitate cross-border personal data flows and allows APEC economies to decide for themselves their domestic levels of personal data protection while facilitating trade and investment in the region.[25]

30 Interoperability between the various personal data protection regimes is also being explored and there have been some promising developments. For instance, the Data Privacy Subgroup of the APEC Electronic Commerce Steering Group has been actively exploring interoperability of the APEC CBPR with the GDPR.[26] Should such discussions be successful, entities could be permitted to make cross-border data transfers within and amongst the two largest geo-economic groupings at the cost of only one set of certifications to the highest applicable standards. This would represent an immense simplification of compliance costs.

31 However, harmonisation efforts will need to be sensitive to the status of the various data privacy regimes, as well as the cultural and socio-political nuances across the different jurisdictions.[27] For instance, while the APEC and ASEAN Privacy Frameworks share similar principles with the GDPR, there are some key differences in their foundational objectives. The APEC and ASEAN Privacy Frameworks emphasise trade and economic growth and therefore seek to avoid unnecessary barriers to information flows and to ensure continued trade and economic growth in their respective regions. In contrast, the GDPR emphasises the fundamental right to data privacy and seeks to enable "free movement of personal data" within the EU while

24 ASEAN Framework on Personal Data Protection (25 November 2016) <https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> (accessed 4 March 2019).

25 ASEAN Framework on Personal Data Protection (25 November 2016) <https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> (accessed 4 March 2019).

26 See, *eg*, "Data Privacy Subgroup Meeting with European Union" *Asia-Pacific Economic Cooperation* <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union> (accessed 4 March 2019).

27 GSMA, "Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC Can Protect Data and Drive Innovation" (September 2018) at p 55.

protecting "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".[28]

32 The free flow of data across borders plays an important role in encouraging innovation, competition and economic and social development in the digital economy. It therefore follows that entities should not see the need to implement high standards of personal data protection as a burden to their business operations. The concept of personal data protection is here to stay. With the general consumer public more cognisant of their rights under personal data protection regimes, and more willing to take action to enforce those rights, businesses who fail to take due care with regard to personal data may well lose more overall in terms of reputational cost for breaches of personal data obligations.

28 General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) Arts 1(2)–1(3).

THE IMPACT ON SINGAPORE ORGANISATIONS ARISING FROM SINGAPORE'S PARTICIPATION IN THE APEC CROSS-BORDER PRIVACY RULES SYSTEM*

Bryan TAN
LLB (National University of Singapore);
Advocate and Solicitor (Singapore), Solicitor (England & Wales);
Partner, Pinsent Masons MPillay LLP

Bernice TIAN
LLB, BSocSc (Singapore Management University);
Associate, MPillay

1 On 20 February 2018, Singapore became the sixth Asia-Pacific Economic Cooperation ("APEC") economy to participate in the APEC Cross-Border Privacy Rules ("CBPR") system, and the second APEC economy to participate in the Privacy Recognition for Processors ("PRP") system.[1] The two systems have the same goal – to harmonise data protection standards across jurisdictions in order to facilitate cross-border data flow for organisations.

2 An examination of the two systems indicates how business organisations that are data controllers and data processors can benefit from Singapore's participation in the CBPR/PRP systems once they are fully implemented.

---

* Any views expressed in this article are the authors' personal views and should not be taken to represent the views of their employer. All errors remain the authors' own.

1 Ministry of Communications and Information, "Factsheet: Singapore joins APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems".

I. APEC Cross-Border Privacy Rules and Privacy Recognition for Processors systems

A. Overview of the systems

3 The CBPR/PRP systems are voluntary, accountability-based systems designed for organisations that are characterised as data controllers and data processors, respectively. Both systems reflect the application of the nine guiding principles that have been set out in the 2004 APEC Privacy Framework to assist APEC economies in developing consistent approaches to domestic personal data privacy and protection standards.[2]

4 As stated in the APEC CBPR/PRP background documents, the primary intent of the CBPR and PRP systems is to promote the ease of cross-border data transfers by harmonising data protection standards across participating economies.[3] On a governmental level, a country wishing to participate in the system must show, to the satisfaction of the APEC Joint Oversight Panel, that it has a comprehensive personal data protection regime which is routinely enforced by a public authority.[4] The personal data laws of each applicant jurisdiction will also be reviewed to ensure that they are consistent with the standards required by the CBPR/PRP systems.

5 Once accepted, participating economies also undertake to create a data protection certification regime, under which public or private entities may register as APEC-recognised accountability agents. Accountability agents are entities tasked with overseeing the implementation and enforcement of the CBPR/PRP systems domestically for interested business organisations, alongside local data protection authorities.

6 There are currently eight participating economies in the APEC CBPR: Australia, Canada, Japan, Mexico, Singapore, South Korea, Taiwan

---

2 APEC Secretariat, "APEC Privacy Framework" (December 2005) <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework> (accessed 15 January 2019).

3 The Cross-Border Privacy Rules and Privacy Recognition for Processors systems' policies, rules and guidelines are available at <http://cbprs.org/documents/> (accessed 14 January 2019).

4 APEC CBPR website, "Economies Requirements" <http://cbprs.org/government/economies-requirements/> (accessed 10 January 2019).

and the US. In Singapore, the Personal Data Protection Commission ("PDPC") is also in the midst of nominating an accountability agent, who will implement the two systems for interested data controllers and data processors to be certified as such.

B. Requirements for certification

7 Both the CBPR and PRP systems consist of the same three-stage process for organisations to obtain certification. First, organisations that are interested in obtaining CBPR/PRP certification conduct a self-assessment of their data protection policies and practices. This self-assessment is based on an APEC-recognised questionnaire, which will be provided to the organisation by the relevant accountability agent. The second stage involves a compliance review of the organisation, to determine whether their policies and practices are indeed consistent with the minimum requirements of the CBPR/PRP systems. In the event that the organisation falls below the standard, it may take the opportunity to make improvements and revisions on the advice of the accountability agent. If the organisation is assessed to be CBPR- or PRP-compliant, its details will be published on a publicly-accessible website directory hosted by the APEC Secretariat. Each listing on the directory will contain contact information of the organisation, its certifying accountability agent, and the relevant enforcement authority. This allows consumers and other interested stakeholders to submit questions and complaints to the appropriate contact person.

8 The final element of the CBPR/PRP systems is that of enforcement. The CBPR/PRP rules are enforced by accountability agents and privacy enforcement authorities – by contract and by law, respectively. Certified organisations which do not comply with the CBPR/PRP programme requirements may have their certification revoked by the accountability agent and may be subject to sanctions by the enforcement authorities. In the event a case involves cross-border or multi-jurisdictional elements, privacy enforcement authorities of participating economies can step up cross-border co-operation efforts through the Cross-Border Privacy Enforcement Arrangement ("CPEA"), which facilitates information sharing, matter referrals and even parallel or joint investigations.

II. Impact of APEC Cross-Border Privacy Rules and Privacy Recognition for Processors on Singapore organisations

A. Increase consumer trust and loyalty

9 The first – and most significant – impact of Singapore's participation in the CBPR/PRP systems is the availability of an independent, international programme that certified businesses can utilise to increase consumer trust. Under the CBPR/PRP systems, businesses that have been certified to be compliant are entitled to display a seal or trust mark to demonstrate their participation in the relevant system.[5] This mark represents a recognition of the organisation's adherence to the data protection standards required under the national laws of the participating economy, which in turn have been assessed to be sufficiently in line with the standards of the APEC CBPR/PRP systems.

10 A 2017 survey conducted by the PDPC found that 66% of people surveyed would lose trust in an organisation if their personal data was shared with other entities without consent.[6] Consequently, if businesses have been certified by third-party assessors to have robust data protection policies and practices in place to safeguard their clients' data, consumers would be more likely to bestow their trust and loyalty. Third-party review and certification can therefore help strengthen the organisation's reputation, building trust and confidence among its consumers.

11 The consistent application of higher data protection standards on an industry-wide level can also further the adoption of new technologies and enable organisations to leverage data as a strategic asset in their business. In particular, the Singapore authorities have often highlighted that having a well-established and competitive data protection regime with industry

5 APEC CBPR website, "Business" < http://cbprs.org/business/> (accessed 10 January 2019).

6 Tan Kiat How, Commissioner of the Personal Data Protection Commission, speech at the Data Protection Seminar and Book Launch (4 October 2018) at para 16.

players that can demonstrate their commitment to comply with these laws is a key element for Singapore's progression as a digital economy.[7]

12 It is also interesting to note that improving consumer trust was similarly cited as the primary rationale for the introduction of the Data Protection Trustmark ("DPTM") certification by the Infocomm Media Development Authority ("IMDA") and the PDPC in July 2018.[8] Much like the CBPR/PRP systems, the DPTM certification scheme aims to "help organisations demonstrate accountable and responsible data protection practices".[9] Business organisations that opt to be certified under the DPTM programme will be entitled to display a DPTM logo in their business communications, to help consumers identify the organisation as one that has been assessed by independent third parties and found to have data protection policies and practices which are compliant with the Personal Data Protection Act 2012[10] ("PDPA").

13 According to the IMDA, the DPTM scheme already incorporates certain elements of the APEC CBPR/PRP systems' requirements and best practices.[11] The two schemes are expected to complement each other once they both come into force, with the effect that Singapore organisations would be able to seamlessly attain both certifications.[12]

---

7 Tan Kiat How, Commissioner of the Personal Data Protection Commission, speech at the Data Protection Seminar and Book Launch (4 October 2018) at para 3.

8 Infocomm Media Development Authority, "Data Protection Trustmark Scheme: Information Kit" at paras 1.3–1.4.

9 Infocomm Media Development Authority, "Data Protection Trustmark Certification" (2 April 2019).

10 Act 26 of 2012.

11 Infocomm Media Development Authority, "Data Protection Trustmark Scheme: Information Kit".

12 Infocomm Media Development Authority, "IMDA and PDPC launch pilot for Data Protection Trustmark certification scheme" <https://www.imda.gov.sg/about/newsroom/media-releases/2018/imda-and-pdpc-launch--pilot-of-data-protection-trustmark-certification-scheme>) (accessed 10 January 2019).

B. Reduce cost of regulatory compliance

14 Organisations with multi-jurisdictional presence would also stand to benefit from the CBPR/PRP schemes, especially if they require cross-border transfers of data in the course of business. Since all participating economies must have a sufficiently comprehensive data protection regime that meets the criteria required under the CBPR/PRP, the data protection requirements of all participating economies are likely to be similar in standard.

15 An organisation that has been certified under the CBPR or the PRP can thus be assured that its data protection policies and practices are also likely to comply with the data protection regulations of *all* economies participating in the CBPR/PRP systems. Obtaining CBPR/PRP certification thus not only provides more clarity and assurance about the regulatory compliance of the organisation's data practices in Singapore and abroad, it may also help with reducing the costs of ensuring compliance with the regulatory requirements under each country's national laws.

16 This is particularly significant for multinational organisations which (a) have a commercial presence in more than one participating economy, and/or (b) require data transfers to entities in other participating economies.

17 Organisations that are present in multiple jurisdictions can use the CBPR/PRP certification to reduce their overall cost of regulatory compliance. If these organisations have a commercial presence in jurisdictions that are also participating economies in the APEC CBPR/PRP, data protection compliance in one CBPR/PRP participating economy would likely be sufficient to achieve compliance in another CBPR/PRP participating economy. Such organisations can thus have a single, uniform set of data policies and practices which are CBPR/PRP-compliant. That set of policies can then be consistently applied across their various offices. This helps reduce the time and financial costs that could otherwise be incurred if the organisation instead had separate policies in each office to comply with the respective national laws.

18 Singapore organisations that are transferring data to foreign entities (whether they are intra-organisation transfers, or transfers to third parties) also have a specific obligation under the PDPA. Section 26 of the PDPA requires that the transferor organisation must take appropriate steps to ensure that the foreign recipient of the data is "bound by legally enforceable obligations … to provide to the transferred personal data a standard of

protection that is at least comparable to the protection under the Act".[13] If the recipient entity is from a CBPR/PRP participating economy (*eg*, the US, Australia) and has already been certified to be CBPR/PRP compliant in that jurisdiction, it is likely that the recipient in question would also be subject to personal data protection obligations under its national laws that are comparable to the PDPA's standards. Consequently, the transferor organisation in Singapore should be able to transfer the data to that recipient in compliance with the recipient's equivalent of the s 26 obligation under the PDPA, without having to carry out a jurisdiction-specific review of the data protection laws of the destination jurisdiction.

C. Improve cross-border data flows

19 Unduly onerous requirements to cross-border data flows are seen as obstacles to electronic commerce, necessitating a World Trade Organization initiative to negotiate trade-related aspects of electronic commerce.[14] On a more general level, the availability of an international certification standard that is used and recognised by multiple countries would also help facilitate the transfer of data among countries. In 2017, it was estimated that data connectivity in the trade industry added approximately 40% to Singapore's gross domestic product.[15]

20 As discussed above, CBPR/PRP certification can provide assurance to organisations that the entity receiving their personal data has appropriate policies and procedures in place that are consistent with both the APEC principles and the laws of their respective countries. As more APEC economies opt to participate in the APEC CBPR/PRP systems, national laws and standards regarding data privacy and protection are likely to grow more harmonised, as economies establish standards that are at least similar

13 See s 26 of the Personal Data Protection Act 2012 (Act 26 of 2012), read together with reg 9(1)(*b*) of the Personal Data Protection Regulations 2014 (S 362/2014).

14 World Trade Organization, "Joint Statement on Electronic Commerce" (25 January 2019) <http://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf> (accessed 22 April 2019).

15 "A Trusted Ecosystem for Data Innovation" *DPO Connect* (August 2017) at p 4 <https://www.pdpc.gov.sg/-/media/Files/PDPC/New_DPO_Connect/aug_2017/pdf/ATrustedEcosystemForDataInnovation.pdf> (accessed 14 January 2019).

to each other in order to meet the APEC requirements. The increasing uniformity helps facilitate the transfer of data among entities in different jurisdictions.

21 For instance, foreign entities from participating economies looking to transfer data to a Singapore entity may have more assurance about the data protection standards under Singapore law if the Singapore entity has been certified to be compliant with the APEC CBPR/PRP systems. Having the APEC CBPR/PRP certification will thus help strengthen the overseas reputation of Singapore CBPR/PRP-certified organisations. Foreign entities will no longer have to ascertain on their own whether each Singapore organisation that they wish to deal with has sound personal data policies and practices; they can instead look on the publicly-accessible APEC directory for Singapore organisations which have been certified to be CBPR- or PRP-compliant.

22 By reducing the number of regulatory barriers in each jurisdiction, CBPR/PRP certification can help facilitate the transfer of personal data across geographical borders. Organisations that have a multi-jurisdictional presence or whose businesses require cross-border data transfers may stand to gain from the increasing harmonisation in personal data protection standards.

III. Conclusion

23 Singapore's participation in the CBPR and PRP systems is a product of the recognition that differing standards of regulatory restrictions across countries have been – and remain – a barrier to free flow of data across geographical borders. Once the CBPR/PRP systems come into force in Singapore, Singapore organisations operating in one or more participating economies will be able to avail themselves of a more cost-efficient method of ensuring their compliance with data protection standards across the region.

24 From an outward-facing perspective, the availability of an independently-assessed certification that an organisation's data policies and practices conform to APEC's standards is a testament – and promise – to consumers that the organisation takes data protection seriously. In the wake of recent personal data breaches both at home and abroad, consumers have grown to value organisations that handle personal data respectfully and

carefully. The resulting increase in consumer trust and loyalty would be extremely beneficial for businesses operating in Singapore.

25 Internally, the availability of the APEC CBPR/PRP certification serves to facilitate both intra- and inter-organisational data transfers that are a part of the organisation's day-to-day operations. Certified organisations will be able to exchange personal data with entities in other participating APEC countries in a seamless way, while maintaining high standards of data protection that comply with the laws of the various jurisdictions in which they operate.

26 Taken together, the increase in consumer trust and reduction in compliance costs can help facilitate data flows across geographical borders. As more economies in the APEC region sign up to participate in the CBPR and PRP systems, it is likely that the harmonisation of data protection standards will continue to expand regionally and internationally.

REGULATION OF CROSS-BORDER DATA FLOW UNDER TRADE AGREEMENTS*

YEOH Lian Chuan†
Managing Director (Sabara Law LLC)

1 It is widely acknowledged by researchers and policymakers that data is a major component of value in traded goods and services. In 2016, the McKinsey Global Institute noted that the value of data flows had overtaken the value of global trade in physical goods.[1] Governments have encouraged the flow of information across borders in the interest of commerce, education, technology and scientific progress. On the other hand, governmental authorities have sought to limit the free flow of information in pursuit of other policy objectives.

I. Evolution of data localisation laws

2 The origins of data localisation can be traced to the dawn of international telegraphy in the mid-19th century, where governments sought to reserve the right to stop the transmission of private telegrams which were deemed to be unsuitable on the grounds of security, public good or morality.[2]

3 The concept of cross-border data flows reached a level of increased global consciousness in the 1970s. This was a period marked by heated global debates about the influence of transnational corporations and 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.

† The author wishes to acknowledge the assistance of Ms Koh Yee Shin and Ms Sheryl Khoo in the preparation of this article.

1 James Manyika *et al*, "Digital Globalization: The New Era of Global Flows" (2016) *McKinsey Global Institute* at p 1.

2 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 4.

comparative technological prowess of the US.[3] Amidst sustained campaigns by global businesses and key governments to place fewer restrictions on corporate data flows, the Organisation for Economic Co-operation and Development ("OECD") adopted its Declaration on Transborder Data Flows.[4] Notably, this document provided an avenue for countries to reach a common consensus on data flow issues.

4 These developments eventually gave rise to a trans-Atlantic axis of tension, with European governments favouring omnibus laws and the establishment of data protection bodies over the US's piecemeal and more permissive approach.[5] This chasm was compounded by the Snowden leaks of 2013, which revealed the extent of US surveillance activities targeting American and foreign citizens. Following the leaks, the governments of several countries, such as Russia and Germany, proposed to introduce requirements that their citizens' online data be hosted locally within the country.[6]

5 Although the motivations for data localisation may be attributable in part to reasons such as individual privacy and national security, some governments have been criticised for using it as a tool to increase local investment and employment opportunities.[7] Indonesia, for example, introduced wide-reaching data localisation measures in 2012 as part of the government's strategy to correct its trade deficit and improve infrastructure. Further, some states equate national sovereignty with data localisation as evidenced by aspects of China's push for "cyber-sovereignty", Russia's

3 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 5.

4 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 8.

5 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 6.

6 Bret Cohen, Britanie Hall & Charlie Wood, "Data Localization Laws and their Impact on Privacy, Data Security and the Global Economy" (2017) 32(1) *Antitrust* 107 at 110.

7 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 3.

approach to its "national Internet segment", and the recently announced "Iranian Internet".[8]

II. Innovative precedent set by Comprehensive and Progressive Agreement for Trans-Pacific Partnership to address data localisation laws

6 Despite the importance of global flows of data, there is currently a lack of widely agreed international regulatory standards. In the absence of meaningful progress at the multilateral level, free trade agreements ("FTAs") have developed new models to address contemporary digital trade barriers. In particular, the 2018 Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP") has set an innovative precedent for addressing data localisation matters.

7 The CPTPP, a trade agreement between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam, may be said to represent the frontier of FTA disciplines on data transfers to date.[9]

8 It is worth noting that CPTPP data rules have already been incorporated into, and influenced, other FTA negotiations which have been launched since the original framework was developed.[10] One example is the recent review of the Singapore–Australia FTA.[11]

9 The CPTPP introduced binding provisions restricting data localisation and imposing requirements on cross-border transfer of data in the Electronic Commerce chapter (Chapter 14) of the CPTPP.[12] The

8 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 8.

9 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 19.

10 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 19.

11 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 19.

12 Andrew D Mitchell & Jarrod Hepburn, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale J L & Tech 182 at 207.

provisions illustrate the parties' underlying commitment to facilitating an open Internet and the free flow of e-commerce across borders.[13] This is well reflected in Art 14.2.1: "The Parties recognise the economic growth and opportunities provided by electronic commerce and the importance of frameworks that promote consumer confidence in electronic commerce and of avoiding unnecessary barriers to its use and development."[14]

10 Articles 14.11 and 14.13 of the CPTPP Electronic Commerce chapter set out a number of specific rules relating to the extent to which businesses may transfer and store data across national borders.[15]

11 Article 14.11, titled "Cross-Border Transfer of Information by Electronic Means", requires CPTPP parties to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business".[16] In effect, this provision facilitates cross-border data flows by enabling service suppliers to transfer business data between the territories of CPTPP parties.[17]

12 Article 14.13, which focuses on the location where data is stored, prohibits a CPTPP party from requiring a business to "use or locate computing facilities in that Party's territory" as a condition for conducting business there.[18] This restricts data localisation measures requiring computing facilities to be stored within a party's territory.[19]

---

13 Andrew D Mitchell & Jarrod Hepburn, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale J L & Tech 182 at 207.

14 Andrew D Mitchell & Jarrod Hepburn, "Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale J L & Tech 182 at 207–208.

15 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 21.

16 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 21.

17 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 21.

18 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 21.

19 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 21.

13 Although the CPTPP has been lauded for its broad and clear support for cross-border data flow, the agreement itself also contains significant exclusions which allow for deviation from the Chapter 14 prohibitions.[20] Should a data localisation measure be challenged under the CPTPP dispute settlement provisions, it appears the exception provisions would likely be pivotal in assessing whether the measure is permitted.

14 One such exclusion lies in para 3 of Art 14.2, which expressly carves out government procurement and government information from the scope of the CPTPP Electronic Commerce chapter.[21] Crucially, it clarifies that the provisions do not prevent a government from requiring any official information, such as critical infrastructure plans, classified policy advice, or social security information, to be stored on servers within a party's territory.[22] Furthermore, the definition of "covered persons" in Art 14.1 of the Electronic Commerce chapter provides for financial institutions an additional exclusion from the Chapter 14 prohibitions.[23]

15 Perhaps the widest exclusion lies in para 3 of Arts 14.11 and 14.13, which clarifies that the CPTPP data rules do not prevent a party from adopting or maintaining inconsistent measures in pursuit of a "legitimate public policy objective". This has the potential to significantly limit the Chapter 14 prohibitions and, by extension, the parties' commitment to facilitating the free flow of e-commerce across borders. Significantly, the article-specific exception replaces the necessity test in the General Agreement on Trade in Services ("GATS") Art XIV with an alternative qualification that a measure cannot impose restrictions "greater than are required" to achieve the policy objective.[24] Given that negotiators opted to use the term "required" rather than "necessary", a tribunal may conclude that CPTPP parties did not intend to apply a necessity standard here, which

20 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 22-23.

21 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 22.

22 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 22.

23 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 23.

24 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 25.

is a standard that was considered by the panel in *U.S.-Gambling*[25] to be relatively high.[26]

16 It is undeniable that the CPTPP provisions are welcome, providing a degree of greater clarity as to the obligations and principles in relation to data transfer than have previously existed under World Trade Organization ("WTO") rules or elsewhere.[27] However, the key restrictions remain subject to open-textured exclusions, just as in the WTO context.[28]

17 Ultimately, the CPTPP reflects the difficulty in making progress on these issues in a plurilateral setting, while implicitly highlighting areas that will need further work if trade law is to better support the digital economy.[29]

III. Uncertainty surrounding applicability of General Agreement on Trade in Services to data flows

18 GATS is a treaty of the WTO that extends the multilateral trading system to the service sector. It may be said to largely predate the pervasive nature of data transfers today. Parties are bound to the extent to which they accept the provisions within and the sectors the agreement applies to. Data localisation "measures relating to cross-border transfer of data are most likely to be examined under GATS, because digital data is usually

25 See World Trade Organization Dispute Settlement, "United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services" (DS285).

26 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 25.

27 Andrew D Mitchell & Jarrod Hepburn, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale J L & Tech 182 at 214.

28 Andrew D Mitchell & Jarrod Hepburn, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale J L & Tech 182 at 214.

29 Andrew D Mitchell & Jarrod Hepburn, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale J L & Tech 182 at 214.

transferred across borders without requiring any transfer of physical commodities".[30]

19 GATS has primarily been applied to "measures affecting trade in services". GATS Art I:2 suggests that GATS applies to digital trade which may be categorised as "cross-border supply" of a service, commonly known as mode 1. Given that cross-border data flows fall under mode 1, it follows that digital services could be said to fall within the ambit of GATS.[31] This is of relevance as countries may find themselves restricted in their implementation of data localisation laws, if they are subject to market access and national treatment obligations due to digital services falling under prior services sectoral commitments.

20 It is important to note, however, that GATS does not unequivocally apply to digital services. There is significant ambiguity regarding which sector digital services may be classified under the Services Sectoral Classification List.[32]

21 There are several key sectors applicable to digital services involving cross-border data flows: *eg*, (a) "computer and related services",[33] (b) "telecommunications services",[34] and (c) "audiovisual services".[35] It is unclear which sector in particular is applicable to digital services. Most WTO members have taken at least partial commitments for the "computer and related services" and "telecommunications services" sectors in their

30 Andrew D Mitchell & Jarrod Hepburn, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale J L & Tech 182 at 196.

31 Joshua D Blume, "Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims against Privacy, Localization, and Cybersecurity Laws" (2018) *Georgetown Journal of International Law* 801 at 807.

32 Andrew D Mitchell & Neha Mishra, "Data at the Docks: Modernizing International Trade Law for the Digital Economy" (2018) 20 Vand J Ent & Tech L 1073 at 1089–1091.

33 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 11.

34 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 11.

35 Mira Burri, "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation" (2017) 51 UC Davis Law Review 65 at 85.

GATS schedules.[36] However, where the sector of "audiovisual services" is concerned, almost no WTO members have made commitments and thus the members remain relatively free to sustain discriminatory measures and adopt new ones.[37]

22 Should digital services be classified under the "computer and related services" or "telecommunications services" sector, WTO members who have made sectoral commitments in these sectors may be subject to market access and national treatment obligations, which would affect the scope and efficacy of data localisation laws.

23 GATS Art XVI: Market Access stipulates that the country must provide access to foreign supplies of a particular sector to its market if it lists a particular sector on its Schedule of Specific Commitments. Footnote 8 of the original document explains that a market-access commitment made in a member's Schedule of Specific Commitments constitutes that member's commitment to the open flow of related services.[38] Thus, data localisation laws could breach a member's mode 1 market-access commitment if they effectively prohibited the cross-border delivery of digital services.[39]

24 GATS Art XVII: National Treatment, on the other hand, requires countries to provide equal market access to foreign and domestic service providers so long as the member lists the service in its Schedule of Specific Commitments.[40] Jurisprudence[41] suggests that determining whether a data localisation measure accords less favourable treatment under Art XVII

36 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 11.

37 Mira Burri, "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation" (2017) 51 UC Davis Law Review 65 at 85–86.

38 Joshua D Blume, "Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims Against Privacy, Localization, and Cybersecurity Laws" (2018) *Georgetown Journal of International Law* 801 at 809.

39 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 13.

40 Joshua D Blume, "Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims Against Privacy, Localization, and Cybersecurity Laws" (2018) *Georgetown Journal of International Law* 801 at 809.

41 World Trade Organization Dispute Settlement: "China–Electronic Payment Services" (DS413) and "Korea–Various Measures on Beef" (DS161).

requires close analysis of the effect and trade impact of the measure.[42] A far-reaching data localisation measure which impedes international trade and is motivated by protectionist impulses is more likely to fall foul of the national treatment obligation than a narrower data localisation measure which targets a legitimate regulatory objective and has a more limited impact on trade.[43]

25 Nevertheless, GATS Art XIV: General Exceptions and Art XIV bis: Security Exceptions may apply.

26 Subparagraphs (a) and (c)(ii) of Art XIV are arguably the most relevant, for they relate to measures necessary to protect "public morals or to maintain public order" and the "privacy of individuals", respectively. It is not difficult to imagine how members may choose to invoke these exceptions to justify data localisation. Nevertheless, the ambit of Art XIV is qualified by a proportionality requirement that a measure must be "necessary" to fulfil the objective of protecting public morals. [44] Given that industry analysts have argued that data security is better achieved through data management and not the storage location of data, it is conceivable that a data localisation measure which does not of itself improve data security could potentially fall short of the necessity test in Art XIV.[45]

27 Further, Art XIV bis may be invoked to defend data localisation on national security grounds.[46] The exception is generally considered to be subjective and self-defining as endorsed by one of the first GATT panel reports, the Panel Report in US–Export Restrictions (Czechoslovakia), which stated that "every country must have the last resort on questions

42 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 14.

43 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 14.

44 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 16.

45 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 17.

46 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 17.

relating to its own security".[47] Nevertheless, members may exercise caution in invoking this exception for fear of establishing unhelpful jurisprudence on the scope of the security exception, or subjecting their national security interests to scrutiny.[48]

28 Fundamentally, the lack of specific provisions addressing data transfers means significant ambiguity prevails with regard to how the existing rules under GATS might be applied to data localisation measures in the event of a dispute.[49]

IV. EU and US divergent approaches to data flows

29 The difficulty in reaching a consistent international regulatory standard and the stalling of negotiations on a multilateral level have led to individual entities seeking to progress negotiations through FTAs.[50] This approach has led to fragmentation of the global consensus towards cross-border data flows. Although both the European Union ("EU") and the US have led worldwide efforts to encourage global information flows, they have adopted fundamentally different approaches to the issue.[51]

30 The EU places greater importance on privacy as a non-negotiable, fundamental human and consumer right under Art 8 of the EU Charter of Fundamental Rights which must be protected by governments.[52] European

47 World Trade Organization, "GATT, United States: Export Restrictions (Czechoslovakia)" (8 June 1949) (Report of the Panel, GATT Doc CP3/SR22 - II/28) at p 3.

48 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 18.

49 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 5.

50 John Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?" (2017) 25(3) *International Journal of Law and Information Technology* 213 at 218.

51 Susan Aaronson, "Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", (2015) 14(4) *World Trade Review* 671 at 675.

52 EU provisions on *Cross-border data flows and protection of personal data and privacy* in the Digital Trade Title of EU trade agreements – explanatory note

(*continued on next page*)

citizens and policymakers support the prohibition of barriers to cross-border data flows to the extent that the EU may maintain its data protection and privacy rules. In the EU, the Snowden leaks triggered memories of communist-era state surveillance.[53] The EU has thus far tried to avoid offering any commitments regarding cross-border information flows or prohibition of localisation provisions in its FTAs.[54] The US, on the other hand, enjoys technological dominance[55] and favours a stronger prohibition on barriers to cross-border data flows in line with its ideals of freedom and liberty.[56] The US Congress, businesses, human rights groups, and many non-governmental organisations ("NGOs") generally support efforts to advance Internet freedom and facilitate the free flow of information.[57]

31 Both the EU and US have sought to promote their respective ideologies through negotiations with their trading partners.

32 The EU, for example, is particularly insistent on retaining regulations which promote privacy and personal data protections. The bilateral EU-Canada Comprehensive Economic and Trade Agreement, for example, includes language in its e-commerce section that "calls for respect of privacy laws, both for the private and public sectors, as well as privacy as a

(5th Round of Trade Negotiations between the European Union and Indonesia) (2018).

53 Susannah Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures" (2018) *World Trade Review* 1 at 3.

54 The 2002 EU-Chile free trade agreement ("FTA") limited itself to soft cooperation pledges in the services chapter, and the EU-Korea FTA does not include language on the free flow of information in the e-commerce chapter.

55 John Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?" (2017) 25(3) *International Journal of Law and Information Technology* 213 at 215.

56 Susan Aaronson, "Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", (2015) 14(4) *World Trade Review* 671 at 687.

57 Susan Aaronson, "Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", (2015) 14(4) *World Trade Review* 671 at 675.

fundamental right".[58] Nevertheless, the EU appears to be open to future commitments to cross-border information flows, as reflected, for example, by Art 8.81 of the EU-Japan Economic Partnership.[59]

33 In negotiating FTAs, the US typically proposes rules that would allow data, as a default, to flow freely across borders.[60] Notably, the separate US-led FTAs with Chile, Singapore, Peru, and Columbia state that signatories should avoid erecting new trade barriers to digital trade, and that neither party may include local presence requirements.[61] Significantly, the US was a participant in the first FTA to include a provision specifically addressing cross-border data flows. This US-Korea FTA contained a soft "best endeavour" style clause for the participating countries to refrain from imposing barriers to information flows.[62] It should be noted that although the US subsequently withdrew from the CPTPP, the binding and substantive provisions relating to data flows within the CPTPP were originally championed by the US.

34 Trade negotiations involving both parties have been plagued by conflict, in part due to their ideological differences with respect to data flows. In 2011, the EU and the US proposed joint language relating to provisions on the free flow of information as part of the negotiations for the

58 Joshua D Blume, "Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims against Privacy, Localization, and Cybersecurity Laws" (2018) *Georgetown Journal of International Law* 801 at 836.

59 Article 8.81 of the EU-Japan Economic Partnership states that "The Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement".

60 Susan Aaronson, "Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", (2015) 14(4) *World Trade Review* 671 at 687–688.

61 Susan Aaronson, "Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", (2015) 14(4) *World Trade Review* 671 at 684.

62 Article 15.8 of the agreement says "the Parties shall endeavour to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders".

Trade in Services Agreement of the WTO.[63] However, as negotiations proceeded, the US disagreed with the EU on specifics: the US wanted an absolute right to transfer information while the EU wanted transfers to be subject to data protection and privacy rules.[64] In spite of strong pressure from the US, the EU has exhibited reluctance to change its position. The parties failed to reach an agreement on data flows, despite signals of the willingness of the US to tolerate the exclusion of audiovisual media services from the scope of the trade deal.[65]

35 Despite both parties' drive to encourage data flows in their own ways, the policies adopted by the US and the EU have arguably made it more challenging for countries to reach a global consensus on the scope of data localisation laws.

V. Other possible mechanisms for the regulation of cross-border data flows

36 Given the concerns with respect to closed intergovernmental processes when negotiating trade agreements, future regulations of cross-border data flows will likely see an increase in multi-stakeholder agreements seeking to promote Internet openness and influence related trade agreements.[66] These multi-stakeholder agreements often feature signatories from many different companies and coalitions that may have the capacity to influence their

63 Susan Aaronson, "Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", (2015) 14(4) *World Trade Review* 671 at 690.

64 Susan Aaronson, "Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", (2015) 14(4) *World Trade Review* 671 at 690.

65 Mira Burri, "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation" (2017) 51 UC Davis Law Review 65 at 121.

66 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at pp 17-18.

governments on these issues.[67] One example is the multi-stakeholder Open Digital Trade Network spearheaded by a coalition comprising over 80 Internet businesses, including leading service providers such as Afilias and Google.[68]

37 Countries may also pursue intergovernmental "soft law" agreements in parallel with their trade agreements to promote cross-border data flows.[69] These agreements are normative frameworks which do not impose sanctions, and actors comply for reasons other than legal constraint.[70] For example, countries at the 2016 G20 summit in China agreed on the need to "develop provisions to discourage local data storage requirements".[71]

38 Finally, countries will likely develop their own national data plans for how public and personal data is to be used and exchanged across borders.[72] The UK, Canada and Australia are all in the process of developing their own data strategies to match their digital trade strategies, and the 99 members of the Open Government Partnership have pledged to develop plans to make public data open to all.[73]

---

67 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 18.

68 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 18.

69 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 19.

70 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 19.

71 William J Drake, Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows (14-15 September 2016, World Economic Forum) at p 19.

72 Susan Ariel Aaronson, "Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows" *Centre for International Governance Innovation* Paper No 197 (November 2018) at p 13.

73 Susan Ariel Aaronson, "Data Is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows" *Centre for International Governance Innovation* Paper No 197 (November 2018) at p 14.

39 In sum, the cross-border flow of data is vital in today's world. Disciplines at the WTO and FTA level exist but are relatively nascent and contain ambiguous exceptions. It is likely, nonetheless, that such provisions will apply in more agreements over time, and in addition measures such as those noted above will continue to be used.

Grounds of Decision

Re Aviva Ltd

[2019] PDP Digest 145

Coram: Tan Kiat How, Commissioner
Case Number: DP-1706-B0860
Decision Citation: [2019] PDP Digest 145; [2018] SGPDPC 4

Personal data *– Disclosure of financial and medical data – Stronger controls needed to protect sensitive personal data*
Protection Obligation *– Disclosure of personal data – Insufficient administrative security arrangements*

19 April 2018

BACKGROUND

1 The Organisation mistakenly sent out by post underwriting letters meant for three different clients (the "Impacted Clients") to another client (the "Recipient Client"). The facts of this matter are uncomplicated and the application of the law is straightforward. Of note, however, is that this incident is disappointingly similar to a prior incident involving the Organisation (see *Re Aviva Ltd*[1] ("*Re Aviva Ltd* [2017]")), for which the Organisation was found to be in breach of s 24 of the Personal Data Protection Act 2012[2] ("PDPA") and fined $6,000.

MATERIAL FACTS

2 The Organisation is a multinational insurance company that offers various types of insurance plans to its policyholders.

3 On 8 June 2017, the Monetary Authority of Singapore ("MAS") informed the Organisation that it had received a complaint on the

1 [2018] PDP Digest 245.
2 Act 26 of 2012.

unauthorised disclosure (the "Incident") as set out at [1] above. The Organisation was unaware of the Incident prior to the notification from MAS. The Organisation in turn notified the Personal Data Protection Commission ("Commission") on 15 June 2017. An investigation was carried out under s 50(1) of the PDPA in relation to a breach of s 24 of the PDPA.

4 The Incident occurred during the enveloping of underwriting letters issued through the Organisation's underwriting department (the "Department") to individual clients who signed up for group insurance policies. Staff in the Department print out underwriting letters to be issued to the Organisation's clients. Each staff will then place the relevant underwriting letter into the case file of each individual client and place the file onto a tray for an administrative staff to pick it up. The relevant administrative staff is to pick up the case files from the trays, remove the underwriting letter, fold it, and seal the underwriting letter in an envelope. The envelope is then placed in the mail basket to be delivered to a postal services company.

5 On the day of the Incident, 1 February 2017, the Department processed about 90 distinct underwriting letters. These underwriting letters were issued to individual clients who had requested for an increase in insurance coverage to update them on the status of their requests. The personal data disclosed in each underwriting letter included an individual's full name, residential address, medical conditions and the sum assured (the "Personal Data").

6 One of the administrative staff (the "Admin Staff") folded four underwriting letters, each of which was addressed to a unique individual client, at the same time. However, the Admin Staff forgot that the letters were meant to be sent to different individuals and enclosed all four letters in a single envelope. As a result, the four underwriting letters were sent to the Recipient Client and the personal data of the three Impacted Clients were disclosed to the Recipient Client when the envelope was opened.

FINDINGS AND ASSESSMENT

Issue for determination

7 The issue to be determined is whether the Organisation had, pursuant to s 24 of the PDPA, put in place reasonable security arrangements to protect the Personal Data from unauthorised disclosure.

8 Section 24 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.

Whether the Organisation was in breach of section 24 of the Personal Data Protection Act

The Personal Data were disclosed without authorisation

9 It is not disputed that the Personal Data fell within the definition of "personal data" under s 2 of the PDPA as it was possible to identify the three Impacted Clients from that information alone.

10 It is also not in dispute that the Personal Data were disclosed mistakenly; the disclosure was therefore without authorisation.

11 Based on the investigations carried out, the Commissioner finds that the unauthorised disclosure of the Personal Data was a result of a breach of the Organisation's obligation to make reasonable security arrangements for the protection of the Personal Data. The reasons for this finding are set out below.

The Organisation relied solely on the administrative staff to perform their duties diligently

12 Upon investigation, it was discovered that there were no processes or safeguards put in place to prevent the Incident. Just as in *Re Aviva Ltd* [2017], the Organisation merely relied on the administrative staff to perform their duties diligently.

13 Random checks on the enveloping carried out by the administrative staff were not conducted. This was despite the fact that a total of four

permanent staff and two temporary staff were tasked to carry out the enveloping of such underwriting letters. It is surprising that none of the four permanent staff were tasked with a supervisory role to conduct random checks. In fact, the Organisation did not have in place any checks on the enveloping work of the administrative staff at any time prior to the dispatch of the letters to individual clients.

14 The Organisation did not even have a process to check if the number of letters sent out corresponded with the number of underwriting letters scheduled to be sent out on the day. This would have been the most basic check and would likely have prevented the Incident, but even this was not conducted. To be clear, it is unlikely that such a basic arrangement on its own would suffice for the purposes of complying with s 24; such an arrangement would still leave potential foreseeable errors (*eg*, one of the pages of a letter being mistakenly included in an envelope to be sent to another individual) unaddressed. It would, however, have been better than nothing.

15 As it was made clear in *Re Aviva Ltd* [2017], relying solely on employees to perform their tasks diligently is not a sufficiently reasonable security arrangement and is a breach of the Organisation's obligation under s 24.

Personal data of a sensitive nature should be safeguarded by a higher level of protection

16 The personal data found in the underwriting letters included data of a sensitive nature such as financial and medical data (*Re Aviva Ltd* [2017] at [17]).

17 All forms or categories of personal data are not equal; organisations need to take into account the sensitivity of the personal data that they handle. In this regard, the Commissioner repeats the explanation in *Re Aviva Ltd* [2017] (at [18]) on the higher standards of protection that should be implemented for sensitive personal data:

> The *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* states that an organisation should 'implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity'. This means that a higher standard of protection is required for more sensitive personal data. More sensitive personal data, such as insurance, medical and financial data, should be accorded a commensurate

level of protection. In addition, the *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* expressly states that documents that contain sensitive personal data should be 'processed and sent with particular care'.

The Organisation encountered a similar incident due to the lack of security arrangements surrounding its enveloping process but failed to take any heed from the prior incident

18 The Organisation's failure to implement any reasonable security arrangements in respect of the enveloping process here is perplexing given the occurrence of a previous incident (the "Prior Incident") suffered by the Organisation and which, as mentioned above, is the subject of the decision in *Re Aviva Ltd* [2017].

19 In the Prior Incident, the Organisation had mistakenly mailed insurance documents which were meant for one policyholder to another policyholder. Just as in the present case, the Organisation relied solely on its administrative staff to perform their duties diligently and had not implemented any security arrangements to prevent the disclosure of personal data arising from the enveloping process.

20 As set out in *Re Aviva Ltd* [2017] (at [37]), the Organisation implemented the following checks as of 3 December 2016 within its processing department to mitigate against enveloping errors:

(a) a random check amounting to a sample size of about 10% would be conducted; and

(b) if an error is detected, the team leader would conduct a 100% audit of the work of the staff who had erred for a period of one week.

21 The investigations show that the above checks were not implemented across all departments within the Organisation. Notably, the Department involved in the present case (*ie*, underwriting department) was not amongst those departments in which the above checks were implemented.

22 If the Organisation did not appreciate the fact that a lack of security arrangements in the enveloping process would potentially lead to an unauthorised disclosure of Personal Data before the occurrence of the Prior Incident, it should have become acutely aware of this potential after the

Prior Incident was reported or at least by the time it had concluded its internal investigations on 3 December 2016.

23 The Organisation had about two months (from 3 December 2016 to 1 February 2017, *ie*, the time of the Incident) to implement some form of security arrangement to prevent the unauthorised disclosure of personal data arising out of mistakes in the enveloping process across its departments. This was, however, not done. In fact, even till as late as 8 June 2017, when MAS notified the Organisation of the Incident, no security arrangements were implemented to prevent such incidents. Clearly the checks which were implemented in respect of the Prior Incident were not complex and could have been rolled out to the rest of the departments within the Organisation which also handled enveloping in a short span of time. In fact, the Organisation had been able to implement some checks as security arrangements (as set out below at [26(d)] and [26(e)] in respect of the enveloping of underwriting letters by 15 June 2017 (within seven days after it became aware of the Incident).

24 Whether or not the checks (described below at [26]) would have prevented the Incident from occurring is beside the point. What is egregious in this case is that the Organisation failed to put in place any security arrangements in the Department, as it was obliged to under the PDPA, to counter the potential of an unauthorised disclosure of personal data through mistakes in the enveloping process even though a similar incident involving an enveloping process within the Organisation had taken place about two months prior to the Incident. By 3 December 2016, the Organisation knew about the process gaps and the need for safeguards arising from its internal investigations into the Prior Incident. Even as it was implementing the recommended safeguards, the Organisation failed to conduct a more thorough review of its internal departments in order to identify more completely those departments that are subject to the same vulnerabilities and risk similar failures as the Prior Incident. It cannot be gainsaid that the Organisation's failure to include the Department in its remedial plans arising from the Prior Incident contributed to the present incident.

25 To be clear, the Commissioner is not making a finding as to the suitability of the above checks as reasonable security arrangements for the work undertaken in the processing and underwriting departments. Neither

is the Commissioner recommending that these checks be implemented throughout the Organisation.

REMEDIATION ACTIONS TAKEN BY THE ORGANISATION

26 The Commissioner notes that after the data breach incident, the Organisation undertook the following remediation actions:

(a) the Recipient Client was contacted and the Organisation procured the return of the underwriting letters addressed to the Impacted Clients;

(b) the Impacted Clients were notified by the Organisation and were given shopping vouchers as a token of the Organisation's apology;

(c) the Organisation emphasised to the administrative staff the importance of checking that the envelopes do not contain letters addressed to multiple individuals;

(d) the Organisation implemented random sampling checks of two envelopes per day and if any enveloping error is detected, a 100% check will be conducted in respect of the enveloping work undertaken by the administrative staff who had erred for one week; and

(e) daily compulsory checks will be conducted to track the number of underwriting letters scheduled to be sent out each day and ensure that it is consistent with the number of envelopes containing these letters to be mailed.

27 As with the Prior Incident, the Commissioner has not reviewed the Organisation's considerations in deciding on the sample size for its random sampling checks and is not providing an opinion on the effectiveness of these random checks. The Commissioner, however, points out that with respect to the follow-up letters which were the subject of the Prior Incident, a random check of two envelopes per day amounted to a sample size of about 10%. Here, given the quantity of underwriting letters the Organisation processed on the day of the Incident (*ie*, 90 letters), the sample size amounts to about 2%.

28 In this regard, the Commissioner reiterates the observation he made in *Re Aviva Ltd* [2017] at [40]–[41]:

40 As a general observation, the Commissioner highlights that organisations should take into account all relevant circumstances and considerations when devising and implementing fresh or enhanced security arrangements in relation to the enveloping process to ensure compliance with s 24 of the PDPA. Such circumstances and considerations include the likelihood of unauthorised access, collection, use, disclosure, copying, modification or disposal of the Personal Data and similar risks in relation to the enveloping process; the sensitivity of the Personal Data and the impact to the individual if an unauthorised person obtained, modified or disposed of the Personal Data; the size of the organisation; and the amount of Personal Data that it is subject to the enveloping process.

41 The Organisation may also wish to consider a graduated approach to sample checking. For example, the enveloping work of new members of staff and members of staff who have recently made mistakes may be subject to stringent checks while the work of senior members of staff with relatively few records of such mistakes may be subject to more moderate checks. It is not automatous checks that are of utmost importance but the efforts that an organisation puts into the development of considered SOPs which focus on the protection of personal data, which in turn contributes to the development of a positive data protection culture amongst its staff.

DIRECTIONS

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

30 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commissioner took into account the following aggravating factors:

(a) the Personal Data disclosed, in particular the medical condition and sum assured, were sensitive in nature;
(b) the Organisation is in the business of handling large volumes of personal data, the disclosure of which may cause exceptional damage, injury or hardship to the affected individuals; and
(c) the Organisation had encountered a similar incident prior to this Incident in which its lack of security arrangements surrounding the enveloping process resulted in the unauthorised disclosure of

personal data of one of the Organisation's clients to another client due to a mistake by an employee of the Organisation during the enveloping process.

31 The Commissioner also took into account the following mitigating factors:

(a) the Organisation had co-operated fully with investigations and was forthcoming in admitting its mistake;
(b) the Organisation had notified the Impacted Clients of the data breach and offered them an apology and shopping vouchers, and had also made arrangements to retrieve the wrongly delivered documents from the Recipient Client;
(c) the unauthorised disclosure of Personal Data was limited to one individual; and
(d) there was no evidence to suggest that there had been any actual loss or damage resulting from the unauthorised disclosure.

32 Pursuant to s 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that the Organisation did not make reasonable security arrangements to protect the Personal Data and is in breach of s 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$30,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

INFORMATION PROVIDED BY THE ORGANISATION SUBSEQUENT TO RECEIVING THE COMMISSIONER'S PRELIMINARY DECISION

33 The Organisation by way of its letter dated 2 March 2018 provided the Commissioner with certain information subsequent to being informed of the Commissioner's preliminary decision that the Organisation was in breach of s 24 of the PDPA and the intention to impose the financial penalty as set out above at [32]. The Commissioner reviewed the information in the said letter and has maintained his views on the matter and his decision to impose a financial penalty, as well as the quantum of the financial penalty.

34 The information provided by the Organisation is summarised as follows:

(a) During the material period, there was a surge in the volume of underwriting letters as the Organisation had successfully bid for a large tender. Prior to the material period the Department had to process 40 letters per day; with the increased sales resulting from the successful bid, the Department had to process about 90 underwriting letters per day.

(b) The administrative staff was trained to carry out the staff's duties including training on the importance of handling personal data.

(c) The Organisation was in the process of implementing a barcoding system for its mail to minimise manual intervention.

(d) The Department was aware of the Prior Incident. According to the Organisation, every function (including the Department) across the Organisation handling personal data was advised to take note of the Prior Incident, assess its processes and consider implementing necessary controls to prevent similar occurrences with each function considering what practices or controls are appropriate for its processes.

(e) The Department assessed that the risk of unauthorised disclosure as a result of its processes and practices was low given that (i) the Department had not suffered such an incident prior to this; (ii) the staff had been sufficiently trained; (iii) there was verification of the clients' names against an underwriting worksheet before the letters were folded; and (iv) they would be implementing a barcoding system.

(f) Reputational damage (if any) on the Impacted Clients would be minimal.

(g) The Organisation took steps to inform the Impacted Clients and apologised for the Incident.

(h) The unauthorised disclosure was limited to one individual.

35 The points summarised above provided an explanation of how the Organisation made its decision and the considerations that it undertook in its risk assessment. The Department made an assessment of the risks and decided not to implement the security measures introduced following the Prior Incident. Clearly, the risk materialised and the Organisation has to be responsible for its consequences.

36 The Organisation's representations concerning its plans to implement a barcode system for processing mail cannot excuse the adoption of the security measures introduced in other parts of the Organisation in the interim since it has continuing obligations to protect its clients' personal data. The future implementation of a barcode system does not address the protection measures that should have been put in place in the interim. It is precisely because of the risk of fluctuating — and in this case, a surge of — workload that interim adoption of the security measures, pending introduction of the barcode system, is necessary.

37 While the Commissioner accepts that personal data protection training which is specific to the administrative staff's role in handling personal data may in certain circumstances be a security measure, it does not detract from the necessity and relevance of operational safeguards in the form of the security measures introduced following the Prior Incident.

38 Pertinently, the Department verified the name of clients against an underwriting worksheet, but this verification was conducted prior to the folding and enveloping of the letters and was not designed to prevent situations similar to both the Incident and Prior Incident where letters were sent to the wrong recipient. More need not be said about the necessity of the Department to have adopted the security measures introduced following the Prior Incident even if to do so was an interim measure pending the implementation of a barcode system.

39 The points set out at [34(f)], [34(g)] and [34(h)] had been already taken into consideration in assessing the quantum of financial penalty to be imposed.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Actxa Pte Ltd

[2019] PDP Digest 156

Coram: Tan Kiat How, Commissioner
Case Number: DP-1611-B0320
Decision Citation: [2019] PDP Digest 156; [2018] SGPDPC 5

Consent Obligation *– Collection, use and disclosure of personal data without consent – Failure to notify individual of purposes for collection and use of personal data – Inadequate privacy policy*
Consent Obligation *– Reliance on deemed consent*
Personal data *– Collection of personal data through mobile application and multiple connected devices (Internet of Things)*
Purpose Limitation Obligation *– Use of personal data without notifying individual of purposes for collection and use of personal data – Inadequate privacy policy*

19 April 2018

BACKGROUND

1 Organisations are increasingly integrating information technology components and computer network connectivity into the products they develop ("connected devices"). The embedded technology and connectivity help turn ordinary products, such as a weighing scale, into a "smart" version of the product with the ability to collect and transfer data wirelessly through the network.

2 These connected devices have the potential to offer a multitude of benefits to improve the lives of users of these devices. A "smart" refrigerator may be able to understand your grocery shopping habits, alert you when you are low on ingredients you commonly use and order these ingredients from an online grocery store and pay for the purchase. A "smart" pacemaker may warn you when you have an impending heart attack, notify the nearest hospital and call for an ambulance.

3 Organisations may use multiple connected devices to collect users' personal data. This would assist organisations in providing an integrated suite of services. As an example, an organisation may collect your body measurements from a "smart" weighing machine and your dietary preferences from your "smart" refrigerator and suggest the amount of daily exercise you should undertake to maintain a healthy body weight through your "smart" watch. Some of these organisations may rely on a single document to notify users of the purposes of, and obtain consent for, the collection, use and disclosure of personal data collected through these connected devices and across different platforms. To be clear, there is nothing wrong with this practice. However, such organisations need to ensure that they comply with their notification and consent obligations across all these different connected devices and any other platforms or sources used to collect personal data.

4 In this matter, Actxa Pte Ltd ("the Organisation"), which sells healthcare and fitness related Internet of Things ("IoT") devices, such as "smart" weighing scales, relied on its website's privacy policy to notify its customers of the purposes, and to obtain the customers' consent, for the collection of personal data across all the Organisation's platforms. The Organisation did not have separate privacy policies, or other documentation, relating to the collection, use and disclosure of personal data collected through the IoT devices it develops and sells.

5 The issue for determination in this case is whether the Organisation, via its website's privacy policy, sufficiently notified its customers of the purposes, and obtained the customers' valid consent, for the collection, use and disclosure of personal data collected through the IoT devices the Organisation develops and sells.

MATERIAL FACTS AND DOCUMENTS

6 The IoT devices which the Organisation develops and sells include (a) a "smart" weighing machine (the "Scale"), marketed under the brand "Sense Smart Scale", that uses bioelectrical impedance analysis technology to measure bone mass, muscle mass, total body fat and total body water, as well as (b) wearable fitness trackers (collectively, the "Fitness Trackers"), marketed under the brands "Actxa Swift" and "Actxa Swift+", that use built-in accelerometers to wirelessly detect movements of the user to track the user's activity levels throughout the day.

7 These IoT devices collect data via sensors fitted to these devices. A user can download and install an app (the "Actxa App") onto his mobile device, create his user account, and link the IoT devices to his user account. Thereafter, the user can access the data collected by the IoT devices through the Actxa App to monitor his health data, such as sleep pattern, heart rate and weight trends. The Actxa App will reflect the data collected by the IoT devices; though the data may also be amended by the user. The data is automatically collected by the Organisation's servers through the Actxa App.

Personal Data collected through the Actxa App and the Internet of Things devices

8 When a user downloads the Actxa App and creates an account, the user will be asked to submit the following personal data via the Actxa App: name; e-mail; password (encrypted); gender; date of birth; height; weight; profile picture (optional); and country ("Personal Data Set A"). This type of personal data is often referred to as declared data.

9 The Scale collects the following personal data: weight; height; body mass index ("BMI"); total body water; total body fat; bone mass; and muscle mass ("Personal Data Set B"). It is possible for the Scale to be used independently of the Actxa App, in which case it will operate as a simple and unconnected weighing scale.

10 The Fitness Trackers collect the following personal data: steps and goal; calories and goal; distance and goal; active minutes and goal; sleep duration and goal; start of sleep (date and time); end of sleep (date and time); sleep duration; and raw sleep data ("Personal Data Set C").

11 Personal Data Sets B and C are typically referred to as observable data as these are collected through sensors either in the Scale or Fitness Trackers. The volume of observable data that is collected through regular usage of the Scale or Fitness Trackers will be much higher than declared data in Personal Data Set A. For convenience the defined terms "Personal Data Set A", "Personal Data Set B" and "Personal Data Set C" will be collectively referred to as "Personal Data" in this decision.

12 At the material time, a total of 2,609 customers had downloaded and used the Actxa App, of which 40 customers were users of the Scale and 2,569 customers were users of the Fitness Trackers.

The Complaint

13 A complaint was made to the Personal Data Protection Commission ("Commission") on 7 November 2016 by an individual (the "Complainant") alleging that the Organisation failed to notify him of, and obtain his consent for, its collection of his personal data.

14 The Complainant's spouse had bought a Scale from the Organisation's website (the "Website") on or around 2 November 2016. The Complainant downloaded the Actxa App, created an account and profile, and started using the Scale around the same time.

15 On 5 November 2016, the Complainant sent an e-mail to the Organisation requesting a refund for the Scale, alleging that the Actxa App transferred the Complainant's personal data to the Organisation's server without the Complainant's knowledge or consent.

16 In response to the Complainant's request, the Organisation deleted the Complainant's account, removed all his personal data from its server, and provided the Complainant with a full refund for the Scale.

The Organisation's Privacy Policy

17 At the time when the complaint was made, the Organisation had a privacy policy that was effective from September 2015 ("Privacy Policy"). All users of the Actxa App ("Actxa App users") were required to agree to this Privacy Policy before they were allowed to use the Actxa App. The Organisation confirmed that all Actxa App users, regardless of which IoT device they were using, were required to agree to the same Privacy Policy. Notably, the Privacy Policy did not contain any references to the collection, use and disclosure of personal data through the Actxa App, Scale or other IoT devices, and instead only referenced the Actxa Website.

18 However, after the complaint was made, the Organisation issued a revised privacy policy which took effect from 13 December 2016 ("Revised Privacy Policy") and included specific references to the Actxa App and details on the types of personal data that it collected, used and disclosed. According to the Organisation, all Actxa App users have been notified of the Revised Privacy Policy via e-mail.

COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

19 The issues to be determined in this case are:

(a) whether the Organisation failed to obtain the consent of the Complainant and other Actxa App users before collecting and/or using their personal data in breach of s 13 of the Personal Data Protection Act 2012[1] ("PDPA") ("Consent Obligation"); and

(b) whether the Organisation failed to collect and use personal data only for purposes that a reasonable person would consider appropriate in the circumstances and for which the affected individual has been informed ("Purpose Limitation Obligation").

Whether the Organisation is in breach of section 13 of the Personal Data Protection Act

20 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.

21 In the present case, the Commissioner is of the view that the Organisation did not obtain valid consent from the Complainant and other Actxa App users to collect Personal Data Sets B and C[2] (collectively referred to as the "Observed Personal Data") and store the said personal data on the Organisation's servers. The Organisation represented to the Commissioner that it collected the Personal Data of the Complainant and other individuals so that the Actxa App would be able to "display, store and retrieve the data and present historical data for the user's consumption".

---

1 Act 26 of 2012.

2 As will be discussed later at [30] to [34], the Actxa App users are deemed to have provided consent for the collection and use of Personal Data Set A by virtue of s 15 of the Personal Data Protection Act 2012 (Act 26 of 2012).

22 The Organisation relies on its Privacy Policy to obtain consent for, and notify the Actxa App users of, the collection, use and disclosure of Personal Data. However, the Privacy Policy only made reference to the Website and did not expressly address the collection, use and disclosure of personal data via the Scale and other IoT Devices through the Actxa App. The first few sentences of the Privacy Policy reads as follows:

> This Privacy Policy discloses the privacy practices for the Actxa *website (collectively, the 'Website' located at www.actxa.com)*. Actxa, the provider of the Website (referred to as 'use' or 'we'), is committed to protecting your privacy online in compliance with Personal Data Protection Ordinance (PDPO) ('PDPO'). Please read the following to learn what information we collect from you (the 'User' or the 'End User') and how we use that information …
>
> …
>
> **Information Gathering**
> Actxa only collects two types of information about our *Website Users*: Personally Identifiable Information and Non-Personally Identifiable Information.
>
> Personally Identifiable Information. Personally Identifiable Information is information that pertains to a specific End Use. The information we collect includes but is not limited to your name, email address, phone number to complete registration. We use this information to provide services and customer support to you.
>
> [emphasis added]

23 There is no mention of the Actxa App throughout the entire Privacy Policy nor any mention of how the Personal Data of Actxa App users may be collected by the Organisation from the Actxa App. The complete absence of any reference to the Actxa App in the Privacy Policy shows that the Privacy Policy was only intended to govern the data collection activities undertaken through the Actxa Website, and not the Actxa App nor the IoT Devices. The opening statement of the Privacy Policy makes express reference to the Actxa Website (and even provides the URL). In addition, the subsequent paragraph in the "Information Gathering" portion of the Privacy Policy refers to information collected from "Website Users" without any reference to users of the Actxa App, Scale and other IoT Devices. From the above, it is clear from the wording that the Privacy Policy was tailored to the Actxa Website, and the Organisation made no effort to adapt the

Privacy Policy to include the personal data protection activities carried out through the Actxa App, Scale and other IoT Devices.

24 The Organisation alleged that since the Privacy Policy would be shown to the Actxa App users prior to their use of the Actxa App, the Actxa App users would have known that the Privacy Policy was applicable to the Actxa App and IoT devices, and not just the Website. However, in the Commissioner's view, this is not an acceptable practice. Displaying a Privacy Policy that has no relevance to the Actxa App cannot amount to proper notification for the Actxa App users, and consent, if any, that is obtained in this manner cannot be valid. It may well be that consent obtained through pretence or obfuscation could amount to a deceptive or misleading practice under s 14(2)(*b*) of the PDPA. To be clear, there is nothing to suggest that in this case, the Organisation was any more culpable than mere omission. Pertinently, it is neither a reasonable nor an acceptable practice to expect individuals who were shown the Privacy Policy to figure out how the Organisation intends for the terms which are tailored to collection of data from the Actxa Website to be adapted for the collection, use or disclosure of personal data via the Actxa App, Scale and other IoT Devices.

25 Compared to declared personal data in Personal Data Set A, the volume, variety and velocity of generation (and collection) of the Observed Personal Data is much higher. The feature set of the Actxa App is non-trivial and likely to become more sophisticated with successive new releases. The use of the Observed Personal Data can also be expected to change in tandem. Accordingly, the purposes for which such personal data will be used should be properly notified to the Actxa App users, in order to obtain their consent. In the circumstances, the Organisation failed to obtain consent from the Actxa App users for, and notify them of, the collection and use of the Observed Personal Data before collection and, thus, the Organisation is in breach of s 13 of the PDPA.

26 Other data protection authorities take similar positions in respect of providing clear notification to users to obtain adequate consent. In Canada, the Office of the Privacy Commissioner of Canada ("OPC"), in a case

relating to targeted advertising, emphasised the importance of providing clear notification for adequate consent by stating the following:[3]

> Organizations must make a reasonable effort to ensure that the individual is advised of the purposes for which their personal information will be used. To make the individual's consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

27 The case above concerned a unique device identifier ("UDID") that was used by Apple Canada Inc ("Apple") and disclosed to third-party app developers via Apple's iOS operating system, for the purpose of delivering targeted advertising to iOS device users. The OPC considered the UDID to be sensitive personal information as it could be used to create a detailed user profile. Although Apple offered easily accessible opt-out options for the use of the UDID with regard to the delivery of targeted advertising, the OPC found Apple's privacy policy to be insufficient as a form of notification as it contained statements which were too broad and generalised. As a result, the OPC recommended Apple to, amongst other things, amend its privacy policy to inform its users in a manner that is "clear, apparent and understandable" how it uses UDIDs to deliver advertising and interest-based ads.[4]

28 In another case, the OPC issued a report of its findings after an investigation into the complaints filed by the Canadian Internet Policy and Public Interest Clinic against Facebook Inc ("Facebook"). The OPC found, *inter alia*, that Facebook had not been clear or specific enough in its notification to its users concerning the collection of a user's date of birth ("DOB") such that the user had the necessary information to make an

---

3 Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2013-017: Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising" (20 November 2013) at "Lessons Learned", fifth bullet point.

4 Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2013-017: Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising" (20 November 2013) at para 48.

informed choice about consent.[5] As such, the OPC required Facebook to amend its privacy policy so as to better explain the purpose for which a user's DOB is collected and used. Facebook was also required to indicate in its pop-up notification that it collected a user's DOB for the purposes of targeted advertising.[6]

29 In the present case, the Commissioner notices that the first line of the Organisation's Privacy Policy makes explicit reference to the "Personal Data Protection Ordinance (PDPO)", which presumably refers to the main data protection legislation in Hong Kong, instead of the PDPA, which is the main data protection legislation in Singapore. This suggests that the Organisation may not have had Singapore data protection law in mind when it was crafting its Privacy Policy. The Commissioner understands that it is common for organisations to adopt a consistent approach across all the jurisdictions in which they have operations and/or presence through privacy policies which apply across jurisdictions. Organisations are reminded that if they choose to adopt such an approach, they should ensure that such privacy policies are compliant with Singapore law.

Is the Complainant deemed to have consented to the collection and use of his personal data?

30 In certain case, an individual may be deemed to have consented to the collection, use and disclosure of his personal data even if he has not actually given consent. Section 15(1) of the PDPA provides that an individual is deemed to have consented to the collection, use or disclosure of his personal data for a purpose if:

---

5 Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2009-008: Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act* by Elizabeth Denham Assistant Privacy Commissioner of Canada" (16 July 2009) at para 51.

6 Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2009-008: Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act* by Elizabeth Denham Assistant Privacy Commissioner of Canada" (16 July 2009) at para 56.

(a) the individual voluntarily provides the personal data to the organisation for that purpose; and
(b) it is reasonable that the individual would do so.

31 In the Commissioner's view, the Complainant could be deemed to have consented to the Organisation collecting, using and disclosing his Personal Data Set A as he had voluntarily entered Personal Data Set A into the Actxa App during the account and profile creation phase and it was reasonable that he would provide the Organisation this personal data for purpose of setting up and managing his account on the Actxa App.

32 However, in respect of Personal Data Set B, whilst the Complainant had used the Scale and Actxa App voluntarily, he was unaware that his Personal Data Set B was being collected by the Organisation and stored on the Organisation's servers. While the state of knowledge of the individual cannot be the limiter on the scope of deemed consent, neither can the purposes for which consent is deemed be so vague or broad that deemed consent ceases to be meaningful. Deemed consent is intended to be relied on in situations where the purpose of collection, use or disclosure of personal data is so clear that the reasonable bystander would have assumed that the individual would ordinarily have provided his consent. Deemed consent is helpful where the transaction is not complex or where it is closely entwined with the performance of an underlying contract. For example, supplying one's payment details and shipping details during an e-commerce transaction, or when engaging a courier to make a delivery. Where the purpose for which consent is provided is clear, the scope of the consent that is deemed can also be reasonably demarcated.

33 In this case, the Commissioner considered the possibility that the features of the Scale and the Actxa App collectively establish the purposes and that consent is deemed for this set of purposes. However, this approach may possibly supplement an inadequate Privacy Policy but cannot be used to construct an absent one for a set of complex functionalities and customer relationship like the present. The feature set of the Actxa App can be expected to change over time and Observed Personal Data will be used in different ways. Further, the relationship between Organisation and customer may last indefinitely, depending on the period of time the customer continues to use the Scale and the Actxa App. These features militate against reliance on deemed consent. In this case, as explained above, there is no Privacy Policy for the Scale or the Actxa App and, for

reasons just provided, deemed consent cannot be relied on to create one by operation of law.

34 Similarly, other Actxa App users may be deemed to have consented to the Organisation's collection, use and disclosure of their Personal Data Set A, but not their Observed Personal Data (depending on which IoT device they use) for the same reasons articulated above. In the circumstances, the Organisation is found to be in breach of the s 13 obligation for failing to obtain consent:

(a) from the Complainant for the collection, use and disclosure of his Personal Data Set B; and

(b) from Actxa App users for the collection and use of Observed Personal Data depending on which IoT device they use.

35 With more developers creating mobile apps, it is unsurprising that guidance has been issued to guide app developers. In the UK, the Information Commissioner's Office ("ICO") has published guidance for mobile app developers, which states that "transparency about purpose is crucial"[7] and sets out important points that developers should take into consideration when drafting notification to users in a mobile environment. In particular, the guidance also highlights how organisations can give their users more control over their privacy such as providing notification when their data is about to be uploaded to the Internet:[8]

> If your app processes personal data in an unexpected way or is of a more sensitive nature you might need to consider the use of additional 'just-in-time' notifications or other alert systems to inform the user what's happening. For example, if geo-location services are running in the background *or you are uploading data to the internet, consider using clear and recognisable icons to indicate that this is occurring and where necessary the option to stop (eg to cancel an upload)*. [emphasis added]

36 The use of just-in-time notifications in order to obtain consent dynamically and in bite-sized portions (as opposed to a lengthy privacy

7 UK Information Commissioner's Office, *Privacy in Mobile Apps: Guidance for App Developers* (December 2013) at p 10.

8 UK Information Commissioner's Office, *Privacy in Mobile Apps: Guidance for App Developers* (December 2013) at p 17.

policy) is one of the ways that the Commission has recommended for adoption in its *Guide to Data Sharing*.[9]

37 Similarly, the Office of the Privacy Commissioner for Personal Data of Hong Kong ("PCPD") has issued an information leaflet in which it highlights the privacy implications that mobile app developers should consider, including the designing of a privacy policy statement:[10]

> ***Privacy Policy Statement (PPS)***
> Apps Developers should prepare a PPS to outline their policies and practices in relation to personal data. Technical terms and elusive language should be avoided in the PPS. *It should be easily readable and easily understandable, and in appropriate length. Its location on the mobile apps should be prominent.* Its availability also on the businesses' normal websites is recommended.
>
> ***Giving examples in PPS***
> *When describing the purposes for which the information is to be used in the PPS, Apps Developers should consider giving real-case examples (as opposed to generic statements) specific to the mobile apps to assist mobile device users in understanding why such information needs to be collected, accessed or shared.*
>
> ***Relevance and Accuracy***
> *Apps Developers should ensure that their PPS are accurate and specific for individual mobile apps. If the description is vague or unclear, the Apps Developers may be perceived as hiding the real purpose of data collection and access. Similarly, if the PPS is copied or extracted from a standard template or another mobile app, Apps Developers have to review the contents to ensure their relevance and accuracy.*
>
> [emphasis added]

38 The Commissioner agrees with many of the general positions taken by the PCPD. In this regard, a privacy policy for a mobile app should, amongst other things:

(a) aim to enhance a user's understanding as to why certain personal data needs to be collected, accessed or shared;

---

9 Personal Data Protection Commission, *Guide to Data Sharing* (27 July 2017) at paras 3.6–3.7.

10 Hong Kong, Office of the Privacy Commissioner for Personal Data, *Personal Data Privacy Protection: What Mobile App Developers and Their Clients Should Know* (November 2012) at p 5.

(b) avoid technical terms and elusive language, be easily readable and understandable, and be of an appropriate length;
(c) be prominently located on the app;
(d) consider using icons and/or just-in-time notifications to obtain specific consent dynamically; and
(e) be reviewed carefully to ensure relevance and accuracy if a standard template is used.

Whether the Organisation is in breach of section 18 of the Personal Data Protection Act

39 Section 18 of the PDPA allows organisations to collect, use and disclose personal data only for purposes which a reasonable person would consider appropriate in the circumstances and for which the affected individual has been notified.

40 Given that the Commissioner has found above, at [25], that the Organisation failed to notify Actxa App users of the collection, use and disclosure of the Observed Personal Data before collecting the said personal data, the Organisation is in breach of s 18 of the PDPA for the same reasons set out above to substantiate a breach of the Organisation's s 13 obligations.

ENFORCEMENT ACTION BY THE COMMISSIONER

41 Given that the Organisation has been found to be in breach of ss 13 and 18 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as it deems fit to ensure the Organisation's compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1m as the Commissioner thinks fit.

42 In assessing the breach and determining the directions to be imposed to the Organisation in this case, the Commissioner took into account the following mitigating factors:

(a) The Organisation had accepted the complaint in good faith and taken prompt steps to broaden the coverage of its Privacy Policy. The Revised Privacy Policy now makes explicit mention of the "Actxa App" and the types of personal data that the Actxa App

would collect from the Actxa App users. Hence, the consent obtained and notification provided by the Organisation is now directly relevant to the Actxa App.

(b) The Organisation had co-operated fully with investigations and was forthcoming in providing information to the Commission.

(c) There were no other complaints received from other Actxa App users, besides the Complainant.

(d) The Organisation had engaged the Complainant in a meaningful manner, and voluntarily offered a refund which the Complainant accepted.

43 The Commissioner also took into account the following aggravating factors:

(a) the breach involved sensitive health-related personal data such as an individual's weight, height, and BMI; and

(b) the personal data of a total of 2,609 Actxa App users were potentially compromised or put at risk.

44 The Commissioner has carefully considered the relevant factors of this case and hereby directs the Organisation to pay a financial penalty of S$6,000 within 30 days from the date of the Commissioner's direction, failing which interest shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Singapore Management University Alumni Association

[2019] PDP Digest 170

Coram: Tan Kiat How, Commissioner
Case Number: DP-1706-B0828
Decision Citation: [2019] PDP Digest 170; [2018] SGPDPC 6

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

30 April 2018

BACKGROUND

1 The Organisation, Singapore Management University Alumni Association, is a registered society under the Societies Act,[1] and is a society which caters to persons who are alumni of the Singapore Management University ("SMU").

2 On 7 June 2017, the Complainant informed the Personal Data Protection Commission (the "Commission") that by entering an identification number (*eg*, NRIC number) on a webpage[2] of the Organisation's website, one could retrieve and access the membership application status and personal data of an individual to whom that identification number relates.

3 On account of the complaint made, an investigation was commenced under s 50 of the Personal Data Protection Act 2012[3] (the "PDPA") to ascertain whether the Organisation had breached its obligations under the PDPA. The material facts of the case are as follows.

---

1 Cap 311, 2014 Rev Ed.

2 At the material time, the URL of the webpage which disclosed the membership application status and personal data was <https://members.smuaa.org.sg/app_smuaa/smuaa-check-application-status>.

3 Act 26 of 2012

MATERIAL FACTS

4 The Organisation introduced the webpage on 28 February 2017 to enable applicants, who had applied to be members of the Organisation, to check the status of their membership application. The webpage was publicly accessible online and the URL of the webpage was also provided by the Organisation to applicants by way of an e-mail. Instructions on how to use the webpage could be found on the Organisation's website.

5 An applicant could, by entering his identification number, specifically either a FIN or NRIC number, onto the webpage, gain access to details associated with his application such as the application status, and also his personal data such as name, identification number, contact number, address, e-mail, and other details relating to his education at SMU (*eg*, graduation year and course).

6 Apart from this requirement to enter an identification number, no other security measures or access controls were implemented to restrict access to personal data of the applicants through the webpage. Hence, from 28 February 2017 until 12 June 2017 (when remedial actions were taken by the Organisation), any person with the identification number of an applicant would have been able to access the personal data of that applicant through the webpage.

7 In contrast, the Organisation indicated that it had comparatively much stronger internal controls for access to the same data in question. The data was stored in its Customer Relationship Management ("CRM") systems and only authorised employees who had been issued individual login credentials could access the data with their credentials.

8 As at 12 June 2017, the personal data of some 297 applicants were rendered accessible through the webpage in such a manner.

9 After receiving notice of the complaint, the Organisation undertook the following remedial actions:

(a) When informed of the complaint on 12 June 2017, the Organisation, on the same day, disabled the webpage to prevent any unauthorised access to the personal data. Subsequently, the Organisation introduced additional requirements of inputting an applicant's e-mail or mobile number (in addition to his identification number) to access his data on the webpage, with the data accessible also reduced to the applicant's application

status, receipt number and date (*ie*, the removal of personal data not otherwise required to ascertain the application status). From 4 July 2017, this feature and the webpage were entirely removed from the Organisation's website.

(b) The Organisation formed a committee to handle all matters relating to the complaint, and also undertook investigations, including a security audit, to determine the extent to which the personal data of the applicants had been compromised for the relevant period between 28 February 2017 and 12 June 2017. The server access logs for the webpage were examined to determine if any persons had exploited the vulnerability of the webpage (in using only an identification number as an access control) to gain unauthorised access to personal data. From the investigation results presented by the Organisation, it appears that it is unlikely that any such unauthorised access had occurred.

(c) The Organisation also represented that it had implemented organisation governance measures to improve PDPA awareness and compliance within the Organisation, including (i) implementing internal operating procedures on data protection; (ii) requiring employees handling personal data to complete the data protection e-learning modules on the Commission's website; and (iii) plans to conduct risk assessment exercises to determine data protection competency.

FINDINGS AND BASIS FOR DETERMINATION

Issues 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 by only securing personal data of the applicants in the manner described in [5] and [6] above.

12 There is no question or dispute that the data in question concerned "personal data" as defined under the PDPA. The data concerned comprised names, identification numbers, contact information and addresses. There is also no question or dispute that the personal data was under the control of the Organisation.

13 The issue that remains is whether the Organisation had taken reasonable security arrangements to protect the personal data concerned, by securing personal data of the applicants in the manner described in [5] and [6] above.

14 In *Re ABR Holdings Limited*[4] ("*Re ABR Holdings*"), it was stated at [16] that:

> … 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.

15 Accordingly, in the case of *Re ABR Holdings*, it was found at [17] that the use of identification numbers to serve the separate functions of identification and authentication to access personal data on the website of a membership programme could not constitute reasonable security arrangements (within the meaning of s 24 of the PDPA) given, amongst other things, that "tools [were] readily available online that can simulate or generate UIN numbers (such as NRIC and birth certificate numbers)".

16 In the present case, the Commissioner for Personal Data Protection ("Commissioner"), following from the decision in *Re ABR Holdings*, likewise finds that securing the personal data of applicants using only identification numbers to serve the functions of identification and authentication to access personal data does not constitute reasonable security arrangements.

17 The Organisation represented that it had instituted internal organisational measures and security standards to protect and restrict access to such personal data within its Organisation (see [7] above). Yet, when it came to protecting and restricting access to the same data from the public, where the risks of unauthorised access is undoubtedly higher, the

4 [2017] PDP Digest 117.

Organisation inexplicably failed to extend at least similar standards of protection, and instead relied on a standard that was much lower. The Organisation itself, in its response to the Commissioner's second Notice to Require Production of Documents and Information ("NTP"), admitted that its use of FIN/NRIC numbers as an individual's sole login credentials for the website was "not a good enough protection as it [would] reveal the full application details of the individual". The Organisation further admitted that the unauthorised access of personal data via its website came about due to the "lack of PDPA knowledge in [its] team".

18 Accordingly, the Commissioner finds that the Organisation has contravened s 24 of the PDPA.

THE COMMISSIONER'S DIRECTIONS

19 Given the Commissioner's findings that the Organisation is in breach of its obligations under s 24 of the PDPA, the Commissioner 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 S$1m.

20 In assessing the breach and determining the directions (if any) to be made, the Commissioner considered, as an aggravating factor, the sensitivity of the personal data involved, which included FIN/NRIC numbers. In this regard, the Organisation made representations intimating that the fact that FIN/NRIC numbers were involved should not have been included as an aggravating factor given that a person trying to access the personal data would have already known the FIN/NRIC numbers. Although the potential population that is at risk is small, the risk to the affected individual is high. Moreover, the use of an NRIC number generation tool would make it relatively easy for a motivated hacker to systematically query the webpage and, if successful, he would have been able to definitively link the NRIC number to the full name, address and other personal data of the member, potentially resulting in significant harm to the individual, such as through identity theft or an unauthorised person impersonating the affected member.

21 The Commissioner also took into account the following mitigating factors:

(a) there was no evidence to suggest there had been any actual loss or damage resulting from the risk of unauthorised access or disclosure of personal data. In this regard, we refer to the server logs provided by the Organisation as set out at [9(b)] above which showed that it was unlikely that any unauthorised access of personal data occurred. The Organisation also confirmed in it its representations that there has been no actual exposure of personal data;

(b) the Organisation had co-operated fully with the investigations; and

(c) the Organisation took prompt action (described in [9]) to remedy the breach when notified.

22 In its representations, the Organisation also asked the Commissioner to consider the alleged obscurity of the website and the difficulty in finding the personal data in question as a mitigating factor. The Commissioner does not view this as a mitigating factor. Once the information is accessible on the Internet, the fact that it may not be immediately found is not by itself a mitigating factor. Instead, what is important is whether there was evidence of actual loss or damage as a result of the incident. The Commissioner had already taken into consideration the lack of actual loss or damage as a mitigating factor in determining the financial penalty quantum in this case before the Organisation submitted its representations.

23 In view of the factors noted above, pursuant to s 29(2) of the PDPA, the Commissioner hereby directs that the Organisation pay a financial penalty of S$5,000 within 30 days of the Commissioner'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 the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

5 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Aventis School of Management Pte Ltd

[2019] PDP Digest 176

Coram: Tan Kiat How, Commissioner
Case Number: DP-1705-B0766
Decision Citation: [2019] PDP Digest 176; [2018] SGPDPC 7

Consent Obligation *– Failure to effect withdrawal of consent*
Consent Obligation *– Failure to obtain consent for new purposes*
Consent Obligation *– Use of personal data without consent – Failure to notify individual of purposes for collection and use of personal data – Inadequate privacy policy*
Purpose Limitation Obligation *– Use of personal data without notifying individual of purposes for collection and use of personal data – Inadequate privacy policy*

30 April 2018

BACKGROUND

1 The present matter concerns an individual (the "Complainant") who had signed up to receive a free brochure for a specific programme organised by the Organisation, but ended up also receiving numerous marketing e-mails from the Organisation that were unrelated to the programme which the individual was interested in. The question raised is whether the Organisation's "use" of the Complainant's personal data to send him the marketing e-mails without his consent is a breach of the Personal Data Protection Act 2012[1] ("PDPA"). In the Commissioner's findings, the answer is in the affirmative.

2 The Commissioner also found that the Organisation had failed to carry out the Complainant's request to remove his e-mail address from the Organisation's mailing list in a timely manner, which led to further

1 Act 26 of 2012.

marketing e-mails being sent to the Complainant after the withdrawal request was made.

3 The Commissioner's findings and grounds of decision of the matter are now set out below.

MATERIAL FACTS

4 The Organisation is an educational institution that collaborates with overseas universities to offer degrees, courses, and programmes to students across various disciplines such as Finance, Marketing, and Business.

5 The Complainant was interested in one of the programmes offered by the Organisation, and submitted his name, e-mail address, and contact number through a web form on the Organisation's website, titled "Take Action Today – Download Free Brochure", at <http://asm.edu.sg/california-state-university> on 12 January 2017.

6 After signing up for this free brochure, the Complainant started receiving marketing e-mails from the Organisation promoting various courses and programmes. For example, one of the marketing e-mails was titled "3 Psychological Discoveries on How to Convert Difficult People into Cooperative Comrades". Another title was "How to Lead and Motivate Multi-Generational Teams through 'Yin' and 'Yang'". The e-mail addresses of the senders were often different for each marketing e-mail, such as "noreply@training-event.net" or "noreply@singapore-event.net". The e-mail addresses did not display a visible association to the Organisation's domain name (as set out in the preceding paragraph).

7 The Complainant then lodged a complaint with the Personal Data Protection Commission ("PDPC") on 15 May 2017, and subsequently provided the PDPC with screenshots or actual samples of 15 such e-mails ("the Marketing E-mails") he had received from the Organisation.[2]

---

2 These 15 Marketing E-mails comprised e-mails from the Organisation that were sent on 5 May 2017; 7 May 2017; another on 7 May 2017; 8 May 2017; 15 May 2017; 18 May 2017; 23 May 2017; another on 23 May 2017; 10 June 2017; 14 June 2017; 15 June 2017; 16 June 2017; 17 June 2017; 18 June 2017; and 19 June 2017.

8 According to the Complainant, he had attempted to unsubscribe from the Marketing E-mails by clicking on the "unsubscribe" hyperlink found in the Marketing E-mails. Additionally, the Complainant had also sent messages to two e-mail addresses, namely "success@aventisglobal.edu.sg" and "shirley@aventisglobal.edu.sg", which were found within the Marketing E-mails, with a request to be removed from the Organisation's mailing list. Between 19 April 2017 and 24 May 2017, the Complainant made a total of five unsubscribe requests, but to no avail.

9 According to the Organisation, it had only received the Complainant's request on 15 May 2017 because the two e-mail addresses that the Complainant had sent his request to were no longer in use by the Organisation, as the e-mail addresses were assigned to a member of staff who had left the Organisation.

10 Following the Complainant's complaint of the matter to the PDPC, the PDPC had also informed the Organisation to remove the Complainant's e-mail address from the mailing list. At that point in time, the Organisation was undergoing a system upgrade and transitioning from its existing customer relationship management ("CRM") system to a new one. Due to a technical and administrative glitch in the process of porting over customer data to the new CRM system, the Complainant's e-mail address was still included in the Organisation's mailing list, causing the Complainant to continue receiving the Marketing E-mails. The Organisation finally corrected this issue in June 2017 and provided confirmation to the PDPC that it had fulfilled the Complainant's request on 21 June 2017.

11 Based on the Commissioner's investigations, the Organisation had used the same web form to collect the personal data of 6,109 individuals and had sent marketing e-mails to 719 other individuals.

FINDINGS AND BASIS FOR DETERMINATION

Issues in this case

12 At the heart of the matter lies the issue of whether the Complainant consented to receive the Marketing E-mails when he submitted his personal details to the Organisation.

13 Section 13 of the PDPA requires that organisations collect, use or disclose personal data about an individual if consent is obtained unless an exception to consent applies. Section 14(1)(*a*) of the PDPA requires that such consent must be given for purposes that have been notified to the individual.

14 Further, s 18 of the PDPA allows organisations to collect, use and disclose personal data only for purposes which a reasonable person would consider appropriate in the circumstances and for which the affected individual has been notified.

15 Given the above, if an organisation were to collect, use or disclose personal data for a purpose different from what an individual has been notified of, or has consented to, then the organisation would be in breach of the consent obligation under s 13 of the PDPA and the purpose limitation obligation under s 18 of the PDPA.

16 The Commissioner also considered whether, even if the Organisation had complied with its obligations under ss 13 and 18 of the PDPA, the Organisation would nevertheless be in breach of s 16(4) of the PDPA. Section 16(4) requires organisations to give effect to the withdrawal of an individual's consent for the collection, use or disclosure of his personal data. This issue arises due to the Organisation's delay in removing the Complainant's e-mail address from its mailing list, which consequently led to the Organisation's continued use of the Complainant's personal data to send him additional Marketing E-mails.

The Organisation did not have valid consent to use the Complainant's personal data to send him the Marketing E-mails

17 According to the Complainant, he had provided his personal data on the web form only for the purposes of receiving a copy of the free brochure from the Organisation to find out more about the specific programme which he was interested in. This consent did not extend to the Organisation being able to *use* the personal data that was collected to send the Complainant the Marketing E-mails which were unrelated to the programme he was interested in. By this reasoning, the Organisation had not complied with s 13 of the PDPA because the Organisation had used his name and e-mail address for a different purpose (*ie*, to send him Marketing E-mails) from which the Complainant had agreed to when submitting his information.

18 The Organisation disagreed with this and provided the PDPC with its website's Terms of Use and Privacy Policy, claiming that the Complainant was sufficiently notified of, and had consented to, the Organisation using his personal data to send him the Marketing E-mails. Having reviewed the Organisation's website (including the web form), Terms of Use and Privacy Policy, the Commissioner did not accept the Organisation's explanation for the following reasons.

The web form did not indicate that the Organisation would use the personal data keyed into the form by individuals to send out the Marketing E-mails

19 The pertinent presentation and content of the web form is as follows:

(a) The title of the web form states "Take Action Today – Download Free Brochure".

(b) This is followed by a line beneath the title which reads: "Kindly fill in the simple form and download a FREE brochure."

(c) Below this line, there are five input boxes, comprising three boxes for a user to input his name, e-mail address, contact number, and two drop-down boxes labelled "Program Interested" and "Specialization".

(d) Right below the last input box, there is a text which reads: "[s]ubmitting this form meant your consent for our representative to contact you."

(e) The last item in the web form is a button labelled "Submit Now" for the user to click to submit the form.

20 To an ordinary user of this web form ("user"), these elements convey that upon submitting the form, the user would have agreed to the Organisation collecting the user's personal data for the purposes (a) of the Organisation providing a free brochure to the interested user, and (b) for a representative of the Organisation to contact the user with regard to the programme which the user was interested in. There is nothing in the web form that suggests that the Organisation intends to use the name, e-mail address or contact number to send out marketing e-mails to the user, in particular marketing e-mails on a subject matter that did not relate to the programme that the user was interested in. In the present case, the information provided did not sufficiently notify the Complainant of these additional purposes and the Complainant cannot be said to have consented

to the Organisation using his personal data for the purpose of sending him the Marketing E-mails.

The Organisation's Privacy Policy allowed the Organisation to use the personal data of the Complainant only for the purposes of providing the Complainant with the brochure of the specific programme he requested and to contact the Complainant in respect of the said programme

21 The Organisation claims that besides the web form, its website's Terms of Use and Privacy Policy also provided valid notification of the purposes for the use of the personal data collected through the web form and thereby had obtained consent for the purposes of sending Marketing E-mails to the Complainant. The Commissioner did not find this explanation satisfactory.

22 The portion of the Privacy Policy found on the Organisation's website pertinent to the collection of the Complainant's personal data through the web form states the following under the section "Information Collected by E-mail and Online Transactions":

> If you send us an e-mail, we will collect your email address and the contents of your message. We will use your email address and the information included in your message to respond to you, to address the issues you identify, and to improve this web site.
>
> We may also use your email address to notify you about updates, services, special events or activities offered by us and our partners. If you would prefer not to receive e-mail or other communications from us, contact us at info@aventisglobal.edu.sg. *If you complete a transaction such as an online application or an information request form, we will collect the information, including personal information that you volunteered in completing the transaction.*
>
> *We will use this information only for purposes for which the transaction was intended.* We may redirect your email message or information you provided through an online transaction to our office other than the one which originally received the message or information in order to better respond to you.
>
> [emphasis added]

23 The reference to "*an online application or an information request form*" includes the web form completed by the Complainant as the web form was essentially a request for further information on a specific programme and

would, therefore, be considered a "transaction" for the purposes of the Privacy Policy.

24 Looking at the pertinent portion of the Privacy Policy, the Organisation has conveyed that it will only use personal data collected as a result of a transaction "for purposes for which the transaction was intended". In this case, the intention in respect of the transaction in question – the provision of personal data in the web form to obtain a brochure on a specific programme – was for the purposes as set out above in [20]. In the circumstances, the consent obtained by the Organisation from the Complainant was for the Organisation to provide a brochure to the Complainant on the specific programme in which he was interested and for a representative of the Organisation to contact the Complainant with regard to the said programme, and not for the purposes of sending Marketing E-mails to the Complainant.

The Organisation's Terms of Use do not apply in respect of personal data collected through the web form

25 While the Organisation's Terms of Use are referred to in the Privacy Policy, the Commissioner is of the view that the Terms of Use do not provide the Organisation with the consent to use the Complainant's personal data for the purposes of sending out Marketing E-mails. The reference to the Terms of Use in the Privacy Policy reads as follows:

> By using the Site, you consent to the collection, use and processing of your personally identifiable information by us in the manner and for the uses described in this Privacy Policy and our *Terms of Use*. We reserve the right to make changes to these policies as appropriate, and will alert you to any changes made. [emphasis added.]

26 Certain portions of the Terms of Use only apply to specific groups of people, *ie*, "Students", "Employees/Staff", and the "General Public". In the present case, the Complainant is neither a student nor employee or staff of the Organisation. As such, the Commissioner has focused on the following portion of the Terms of Use applicable to the "General Public" in determining whether consent had been obtained from the Complainant to allow the Organisation to send Marketing E-mails to him:

> **Purpose for the Collection, Use & Disclosure of Personal Data**
> *Depending on your relationship with us*, the personal data which we collect from you may be used and/or disclosed for the following purpose:

For General Public

AVENTIS as an educational institution often organise a myriad of training, upgrading and career related activities in which general public are invited to participate. While it is impossible to list all the events in which we hope the public will participate, some events that you as a member of the public can look forward to include corporate outreach programmes, seminars, workshops, talks, exhibitions, etc. Naturally, in encouraging a vibrant interaction with the public, there will be opportunity, and often a need, to collect, use and/or disclose personal data from members of the public.

The key reasons are as follows:

- For verification purposes for Events
- For administrative purposes for certain Events
- To keep you updated of future Aventis Events/products which we feel may interest you
- For marketing/publicity purposes
- For any other purpose arising in respect of the environment within which an institution of higher learning such as AVENTIS operates which is reasonable given your relationship with AVENTIS

In almost all of the above situations, it will be up to you as to whether, and to what extent, you wish to provide us with your personal data. *Typical data collected include participant's name, email and phone numbers.* Based on the information provided, the general public may be contacted by various channels including through social media, Whatsapp, emails, phone calls, postal mail, electronic mail, SMS and/or voice calls; …

[emphasis added]

27 While the Organisation's Terms of Use as set out above do refer to the use of personal data for the purposes of keeping users updated of future events and products as well as for marketing and publicity purposes, the Terms of Use, unlike the Privacy Policy, do not mention the collection of personal data online, either through any online application, information request form, or web forms. Applying the legal maxim *generalia non specialibus derogant* (*ie*, where a contract contains general terms and specific terms, the specific terms are to be given greater weight than the general terms if there is a conflict between the two[3]), the Commissioner finds that greater weight should be given to the Privacy Policy which specifically deals with the purposes for which personal data collected through the web form

3 Kim Lewison, *The Interpretation of Contracts* (Sweet & Maxwell, 6th Ed, 2015) at para 7.05.

would be used. The provisions in the Terms of Use would be inconsistent with the Privacy Policy if the Terms of Use are generally applicable to personal data collected through the web form.

28 Accordingly, in the Commissioner's findings, the Organisation did not provide notification of the purposes for which the marketing e-mails were sent out, and consequently, the Complainant also did not provide consent to his personal data being used for such purposes. The observations made above are equally applicable in respect of the Organisation's failure to limit the use of the Complainant's personal data to the notified purposes. In the circumstances, the Organisation is in breach of ss 13 and 18 of the PDPA.

Even if the Organisation had consented to the sending of the Marketing E-mails, it failed to give effect to the Complainant's withdrawal of consent

29 In the case at hand, even if the Organisation had obtained the requisite consent and provided the relevant notification, the Organisation would have nevertheless failed to comply with s 16(4) of the PDPA as it did not give effect to the Complainant's withdrawal of consent within a reasonable time.

30 In this regard, the unsubscribe requests and the e-mails from the Complainant requesting to be removed from the Organisation's mailing list (as set out in [8] above) as well as the same request made through the PDPC (as set out in [10] above) would have all, individually, triggered the Organisation's obligation to give effect to the Complainant's withdrawal of consent. These requests were sent between 19 April 2017 and 24 May 2017. However, the Organisation only fulfilled the Complainant's request in June 2017; with the PDPC receiving confirmation of this from the Organisation on 21 June 2017. The Organisation admitted to receiving the Complainant's e-mails at least by 15 May 2017. It took the Organisation about a month to effect the Complainant's request to be removed from the Organisation's mailing list from the time it admitted to receiving the Complainant's request.

31 This runs afoul of the obligation under s 16(4) of the PDPA which requires organisations to put in place accessible means for data subjects to be able to withdraw consent to the collection, use and disclosure of their personal data.

32 As stated in the PDPC's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*,[4] as a general rule of thumb, organisations should give effect to a withdrawal notice within ten (10) business days.[5] Should the organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame by which the withdrawal of consent will take place.

33 Accordingly, given that the Organisation has taken such a long time to give effect to the withdrawal of consent to use the Complainant's personal data to send the Marketing E-mails, the Commissioner is also of the view that the Organisation has, in the alternative, failed to comply with s 16(4) of the PDPA.

34 Before leaving the discussion on the Organisation's s 16 obligation, the Commissioner notes that the unsubscribe facility provided for in the Organisation's Marketing E-mails was included to comply with s 11 of the Spam Control Act[6] ("Spam Control Act") which states that:

> Any person who sends, causes to be sent or authorises the sending of unsolicited commercial electronic messages in bulk shall comply with the requirements in the Second Schedule.

35 The Second Schedule provides that every unsolicited commercial electronic message (such as marketing e-mails sent in bulk without having obtained the consent of the individual recipients) shall contain a method for the recipients to unsubscribe from receiving such electronic messages in the future.[7] The sender is not allowed to send any further unsolicited commercial electronic messages to recipients who have unsubscribed after the expiration of ten business days after the day on which the unsubscribe request was submitted.[8]

36 The Commissioner is of the view that any recipient of a marketing e-mail who submits an unsubscribe request using the unsubscribe facility provided by the sender of the marketing e-mail (as required by the Spam Control Act) provides notice to the sending organisation, for the purposes

---

4 Revised 27 July 2017.

5 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 12.42.

6 Cap 311A, 2008 Rev Ed.

7 Spam Control Act (Cap 311A, 2008 Rev Ed) Second Schedule, para 2(1).

8 Spam Control Act (Cap 311A, 2008 Rev Ed) Second Schedule, para 2(7).

of the PDPA, of the recipient's withdrawal of consent in respect of the use of the recipient's personal data for the purposes of sending the recipient marketing e-mails.

37 Organisations should therefore be aware that the unsubscribe facility serves a twofold purpose – (a) compliance with s 11 of the Spam Control Act, and (b) as a way for an individual recipient of marketing e-mails to provide notice to the sending organisation of his withdrawal of consent to the use or disclosure of his personal data for the purposes of sending him marketing e-mails, in accordance with s 16 of the PDPA. A failure to give effect to an unsubscribe request may lead to a breach of s 11 of the Spam Control Act and, as in this case, a breach of s 16(4) of the PDPA.

38 For the avoidance of doubt, the Commissioner is not making any determination in respect of the Organisation's compliance with its obligations under s 11 of the Spam Control Act as such disputes are within the jurisdiction of the courts.

ENFORCEMENT ACTION BY THE COMMISSIONER

39 Given the Commissioner's findings that the Organisation is in breach of its obligations under the PDPA, the Commissioner 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 S$1m.

40 In assessing the breach and determining the directions to be made, the Commissioner considered, as an aggravating factor, the fact that the Organisation had failed to take timely or reasonable steps to resolve or remediate the matter, despite receiving multiple requests from both the Complainant and the PDPC. Another aggravating factor the Commissioner took into account was the high number of affected individuals; the Organisation had used the same web form to collect the personal data of 6,109 individuals, out of which 719 individuals had received similar marketing e-mails not specific to the programmes that these individuals were interested in from the Organisation.

41 The Commissioner also considered, as a mitigating factor, the fact that the Organisation has been generally co-operative with the investigation and provided its responses to the PDPC's questions promptly.

42 The Commissioner hereby directs the Organisation to pay a financial penalty of S$12,500 within 30 days from the date of the Commissioner's direction. Additionally, the Organisation is directed to carry out the following within 30 days:

(a) cease the use of personal data about individuals for purposes which the individuals have not been notified; and
(b) review its procedures and processes for the withdrawal of consent by individuals to ensure that such withdrawals are effected upon the receipt of reasonable notice.

REPRESENTATIONS BY THE ORGANISATION

43 The Organisation submitted its representations by way of a letter dated 5 April 2018 from its solicitors. The Organisation indicated that the Commissioner should consider its track record of acting in accordance with unsubscribe requests, that it acted quickly to improve its administration of unsubscribe requests by on-boarding a new platform to deal with such unsubscribe requests and that the delay in responding to the Complainant's unsubscribe request was due to its migration to the new platform which is a one-off occurrence. The Organisation also indicated that it had not received the initial unsubscribe requests of the Complainant.

44 The Commissioner is of the view that the above representations do not warrant a reduction in the penalty imposed for the following reasons:

(a) The Organisation has not adduced any evidence to show that it has a track record of acting in accordance with unsubscribe requests. In any event, even if it was able to show the same, the main finding here is that there was a breach of the consent obligation. Complying with the wishes of individuals to be unsubscribed from mailing lists does not address the main finding that the Organisation collected and used personal data for purposes for which the Complainant did not consent to in the first place. At most, it is a remediation of its initial breach.
(b) While the Organisation may have on-boarded a new platform to better comply with its obligations to give effect to a withdrawal of consent, the Organisation took about a month to give effect to the Complainant's wishes to be removed from its mailing list. While the Organisation has attempted to explain this by

claiming that this delay was caused by the on-boarding of the new platform, the Organisation should have put in place measures in the interim to ensure that the Complainant did not receive any further marketing material from the Organisation.

(c) The Commissioner had already given the Organisation the benefit of the doubt with respect to the date on which it became aware of the unsubscribe requests and based his findings and the determination of the penalty quantum on the Organisation's agreement that it at least became aware of the Complainant's unsubscribe request on 15 May 2017.

45 The Organisation also sought to compare the penalty imposed against them with previous cases. The Commissioner highlights that the penalty imposed in each case is based on the facts in each case and is only arrived at after a detailed consideration of the facts in each case and a comparison with past cases which are broadly similar. In this case, given the aggravating and mitigating factors present as set out at [40] and [41] above, the Commissioner decided that a penalty of $12,500 was warranted.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re AIG Asia Pacific Insurance Pte Ltd

[2019] PDP Digest 189

Coram: Tan Kiat How, Commissioner
Case Number: DP-1707-B0901
Decision Citation: [2019] PDP Digest 189; [2018] SGPDPC 8

Definition of "control"
Definition of "possession"
Protection Obligation *– Disclosure of personal data – Insufficient administrative security arrangements*

3 May 2018

BACKGROUND

1 On 30 June 2017, the Personal Data Protection Commission (the "Commission") received a data breach notification from the Organisation, AIG Asia Pacific Insurance Pte Ltd (the "Organisation" or "AIG"), informing the Commission that:

(a) the personal data of some of the Organisation's policyholders (for its Individual Personal Accident product) had been compromised and disclosed to an unauthorised party (the "Unauthorised Disclosure"); and

(b) the Unauthorised Disclosure had occurred because the Organisation had stipulated an incorrect facsimile number on the policy renewal notices issued to its policyholders, which had caused its policyholders to fax their renewal notices to a third party, Tokyu Hands Singapore Pte Ltd ("Tokyu Hands") instead of the Organisation.

2 On account of the notification made, the Commissioner commenced an investigation under s 50 of the Personal Data Protection Act 2012[1] (the "PDPA") to ascertain whether the Organisation had breached its obligations under the PDPA. The Commissioner's findings and decision are set out below.

MATERIAL FACTS

3 The Organisation is a general insurance company, and among the largest general insurance companies in Singapore.

4 The Organisation implemented a new electronic policy administration system on 29 November 2016. This system was responsible for generating forms including for its Individual Personal Accident product. These forms included the quote application form, endorsement quote form, policy schedule, endorsement schedule and renewal notice.

5 The form which is the subject of the data breach notification is the renewal notice. The renewal notice is a form that is generated by the Organisation and sent to a policyholder to notify the policyholder on policy renewal and to facilitate the policyholder renewing his or her policy. The policyholder can renew his or her policy by endorsing the renewal notice and returning it to the Organisation.

6 The renewal notice generated by the Organisation contains personal data of the policyholder including the policyholder's name, address and policy details as well as, depending on the policy, personal data of the policyholder's family members (the "Personal Data"). The renewal notice also contains a section which allows policyholders to provide their updated personal data such as updated address, e-mail address and/or telephone numbers to the Organisation, as well as their payment details.

7 From 29 November 2016 (when the new system was implemented) until 19 May 2017, an incorrect facsimile number was indicated on all the forms generated by the system for the Individual Personal Accident product, including the renewal notice. This incorrect facsimile number was provided by a member of the Organisation's staff during the development of template forms for the system. This incorrect facsimile number was

1 Act 26 of 2012.

formerly in use by the Organisation prior to 11 March 2011 but is now in use by Tokyu Hands.

8 As a result of the incorrect facsimile number, policyholders who were sending and returning their renewal notices to the Organisation during this period by facsimile had their renewal notices sent to Tokyu Hands instead of the Organisation.

9 The incorrect facsimile number was (fortuitously) corrected when the Organisation conducted a standardisation exercise on its system to ensure that the same contact information was provided across the Organisation's different forms for different products. Even then, the Organisation did not realise that there had been an error in the facsimile previously provided. It was only on 29 May 2017 that the Organisation became aware of the error after receiving notice from Tokyu Hands that it had been receiving the renewal notices intended for the Organisation.

10 The Organisation informed the Commission that Tokyu Hands had received approximately one to five facsimiles weekly that were intended for the Organisation. In other words, for the period from 29 November 2016 to 29 May 2017, between 25 and 125 renewal notices intended for the Organisation could have been sent to Tokyu Hands. It also appears that the majority of these renewal notices had been sent by the Organisation's own agents (on behalf of its policyholders).

11 The renewal notice with the incorrect facsimile number had been in circulation for a period of six months. In this regard, even after the notices were corrected, Tokyu Hands continued to receive renewal notices intended for the Organisation by facsimile, with 11 such notices received between 30 May 2017 and 25 July 2017. Such risk would of course reduce with the passage of time. In this regard, the Organisation had in its representations, by way of its letter of 5 April 2018, confirmed that any outstanding renewal notices have by now lapsed and, as such, it is unlikely that any further renewal notices would be faxed to the wrong number. Given the process put in place between the Organisation and Tokyu Hands to contain the breach, any possibility of further renewal notices being faxed to Tokyu Hands was not considered in determining the quantum of financial penalty to be imposed. Nonetheless, there was no reduction of the financial penalty on the basis of the Organisation's confirmation that the renewal notices have since lapsed.

12 In addition to correcting the facsimile number, the Organisation has since taken additional steps to address the data breach and the impact on affected policyholders:

(a) the Organisation has sought and obtained confirmation from Tokyu Hands that it has either destroyed or returned to the Organisation, all renewal notices received by Tokyu Hands, and that no copies of such notices have been retained;
(b) the Organisation has made arrangements to contact Tokyu Hands on a bi-weekly basis, and to collect any renewal notices that may have been sent to Tokyu Hands;
(c) the Organisation had on 1 June 2017, communicated to all its producers and agents, the correct facsimile number to be used;
(d) the Organisation is (or will be) undertaking a thorough review of all other forms used in its system to ensure that the contact and facsimile numbers are correct; and
(e) the Organisation has taken steps to reverse any negative impact on the policies of policyholders who had sent their renewal notices to Tokyu Hands instead of the Organisation (*eg*, lapsed policies due to late renewal submissions have been backdated and renewed).

13 The Organisation has also put in place measures to reduce the risks of a similar incident by:

(a) requiring its managers to verify the accuracy of contact information collated by its staff; and
(b) including in the user acceptance testing process for its systems, a step to confirm that documents sent using the contact details provided by the Organisation is received by the intended recipient.

COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

Issues to be determined

14 An investigation was conducted into the unauthorised disclosure. The issue in the present case is whether the Organisation had breached s 24 of the PDPA in providing an erroneous facsimile number on the renewal

notices to which policyholders were to fax the duly completed renewal notices, resulting in the notices (and the personal data contained therein) being sent to an unauthorised third party.

15 There is no question or dispute that the data in the renewal notice is "personal data" as defined under the PDPA. The data concerned comprised names, addresses, policy details, payment details and contact details of policyholders. There is also no question or dispute that the PDPA applies to the Organisation as it falls within the PDPA's definition of "organisation".

The Organisation was in control or possession of the Personal Data

16 Taking the formulation of the elements of a breach of s 24 of the PDPA from *Re Hazel Florist & Gifts Pte Ltd*,[2] the next question to be asked is whether the Personal Data is in possession or control of the Organisation such that the obligation to make reasonable security arrangements attaches in respect of the Personal Data.

17 The Organisation was in *possession* of the Personal Data for the following reasons. First, it had the Personal Data of each of the affected individuals on record as each of them had an existing relationship with the Organisation. Second, it generated the renewal notices with the Personal Data pre-filled such that the individual need only sign the renewal notice and return it by facsimile transmission. It is only where there had been changes to the Personal Data on record that the individual had to provide updated information.

18 The Organisation was also in *control* of the Personal Data. While there is no definition of "control" in the PDPA, the meaning of control in the context of data protection is generally understood to cover the ability, right or authority to determine (a) the purposes for; and/or (b) the manner in which personal data is processed, collected, used or disclosed.

19 In this regard, the Hong Kong Administrative Appeals Board, in the case of *Shi Tao v The Privacy Commissioner for Personal Data*,[3] agreed with the view of the Hong Kong Privacy Commissioner for Personal Data that control "can either mean the physical act of collecting, holding, processing

2 [2018] PDP Digest 199 at [8].

3 Administrative Appeal No 16 of 2007.

or using the personal data or it can mean the ability of determining the purpose for which or the manner in which the data are to be collected, held, processed or used". Further, the UK Information Commissioner's Office ("ICO"), in its guidance[4] on the difference between data controllers and data processors, stated that "[t]he data controller determines the purposes for which and the manner in which personal data is processed. It can do this either on its own or jointly or in common with other organisations. This means that the data controller exercises overall control over the 'why' and the 'how' of a data processing activity".

20 It is clear that the Organisation which collected, processed and used the Personal Data for the purposes of providing its clients with insurance services was in control of the Personal Data. The Organisation determined what personal data it required to provide its services and the purposes for, and the manner in, which the Personal Data was collected, processed, used and disclosed. This is not in dispute. In particular, the Organisation was in a position to decide, and did in fact do so, that as a matter of providing a better experience to its customers when renewing their policies, it pre-filled the renewal notices with each customer's Personal Data on record. This clearly demonstrates the Organisation's control of the Personal Data.

21 Given that AIG is an organisation within the definition of the PDPA and that it is in possession and control of the Personal Data, s 24 of the PDPA applies to it in respect of the Personal Data.

22 However, before assessing whether the Organisation had made reasonable security arrangements to protect the Personal Data, the Commissioner, for completeness, assessed whether the Organisation was in control of the payment details and updated contact details which were entered into the renewal notice by, or on behalf of, the individual policyholders after the renewal notices left the Organisation's actual possession.

23 In this regard, in *Re The Cellar Door Pte Ltd*,[5] it was found that there is a distinction between the possession and control of personal data and that an organisation that does not possess personal data may still be in control of

4 UK Information Commissioner's Office, *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* (6 May 2014) at para 15.

5 [2017] PDP Digest 160.

the personal data (albeit in that case, the personal data was processed by a data intermediary on behalf of the organisation).

24 In the present case, the Organisation designed the renewal notice, pre-filled in the forms with relevant data including the Personal Data and stipulated the fields in the renewal notice which the individual policyholders were supposed to fill up, including the payment details and the updated contact details. The Organisation also devised the process for which policyholders may renew their insurance policies by faxing the duly completed renewal notice to the facsimile number it provided. Therefore, the Organisation was solely responsible for determining the purposes for which the payment details and updated contact details were collected, processed and used and directing the manner and mode of transmitting the renewal notice (and the Personal Data contained therein). Therefore, in so far as the policyholders were transmitting the renewal notices (and their personal data) in accordance with the Organisation's instructions, such Personal Data was within the Organisation's control at the material time (*ie*, when the personal data was filled in and faxed to the erroneous facsimile number).

25 The Commissioner therefore finds that the Organisation was in possession and control of the Personal Data (including the payment details and the updated contact details where such data was filled in by policyholders) within the meaning of s 24 of the PDPA.

26 The final issue that remains is whether the Organisation had taken reasonable security arrangements to protect the Personal Data concerned, when the Personal Data was in the Organisation's possession and control.

Whether reasonable security arrangements taken by the Organisation

27 The fact that personal data had been disclosed to an unauthorised party by an error or flaw in an organisation's systems and processes does not automatically mean that the organisation is liable under s 24 of the PDPA for failing to take reasonable security arrangements to protect personal data.

28 For the purposes of s 24, the Commissioner has to consider what security arrangements (if any) an organisation had implemented to prevent such unauthorised disclosure, and whether those arrangements are reasonable.

29 In this case, the Organisation failed to stipulate the correct facsimile number to which the duly completed renewal notices were to be sent. Such a failure would necessarily (and did) result in the notices being sent and disclosed to an unauthorised third party to whom the incorrect facsimile number belongs. The issue is therefore whether the Organisation had taken reasonable arrangements to prevent an unauthorised disclosure of the Personal Data through the stipulation of an incorrect facsimile number.

30 The investigations found that the Organisation did not have any security arrangements to prevent such unauthorised disclosure. In particular, the Organisation did not have any arrangement or process to verify the accuracy of facsimile numbers uploaded or in use by its systems (and in the forms generated by its system). The Organisation clarified in its representations that it relied on the facsimile numbers provided by the relevant departments within the Organisation when entering the numbers into the new system and verifying that the numbers keyed in matched the numbers provided by the relevant departments. There was, however, no check to verify that the facsimile numbers were up to date. When the system was developed and tested, the scope of the testing only involved a verification that the facsimile number in the template forms (which was then incorrect) corresponded with the forms generated by the system. Also, the user acceptance testing process did not provide for the tester to send a test fax to the facsimile number to verify that the document was received.

31 This failure to undertake any verification is particularly alarming given that the incorrect facsimile number had not been in use by the Organisation for over five years by the time it was uploaded into the system. The incorrect facsimile number was (fortuitously) corrected almost six months after the system was operative, without the Organisation realising that there had been an error. The Commissioner is of the view that merely verifying the facsimile numbers entered into the system against the facsimile numbers provided by the relevant departments was wholly insufficient as a security arrangement and did not warrant a reduction in the penalty imposed. In fact, had the foregoing verification also not been present, the Commissioner may have increased the penalty imposed, as it would show a very grave lack of basic information security practices.

32 The Commissioner also takes the view that it is only reasonable for a company like the Organisation to have some arrangement to ensure that the contact details it provides for the purposes of receiving personal data are

accurate. As a general insurer, the Organisation receives a large volume of documents containing personal data of its many existing and prospective policyholders. It is therefore incumbent on the Organisation to stipulate correct and updated contact details (and ensure that it has done so) to avoid the risk of such personal data being sent to an unauthorised third party instead (as in the present case).

33 One of the considerations that an organisation should factor into its information security arrangements is the monitoring of its systems and processes to detect potential data security breaches (such monitoring to detect data security breaches will be referred to as "data security monitoring"). In this regard, the Organisation intimated that it does monitor its renewal business but that its monitoring did not indicate any significant deviation. It is not clear whether the Organisation monitored the number of renewal notices it received by fax (which was the suggestion by the Commissioner) as opposed to the general renewal business (including renewals by other means and not just by way of facsimile). The monitoring of the general renewal business would not constitute data security monitoring; instead this is generally done for business reasons and any data security aspect would be incidental. However, the monitoring of the number of renewal notices received by facsimile may constitute a data security monitoring measure. To be clear, such a data security monitoring measure would not have prevented the unauthorised disclosure or a finding of breach given the facts of this matter. Any such data security monitoring measure would, nevertheless, be imperative in containing any unauthorised disclosure. The monitoring of the number of renewal notices received by facsimile would have been a very basic and relatively inexpensive form of data security monitoring and would have, likely, only provided sufficient feedback after a significant period. In the circumstances and considering all the facts of this case and the Organisation's representations, the Commissioner is of the view that the penalty imposed in this case (set out at [38] below) is warranted and maintains his decision on the quantum of the penalty.

34 The Organisation has maintained that the data breach arose due to inadvertent human error. As it has been noted on a number of occasions

(including in *Re Social Metric Pte Ltd*[6]), inadvertent human error is not a valid reason for an organisation failing to comply with s 24 of the PDPA.

35 Accordingly, the Commissioner finds that the Organisation has breached s 24 of the PDPA.

THE COMMISSIONER'S DIRECTIONS

36 Given the Commissioner's findings that the Organisation is in breach of its obligations under s 24 of the PDPA, the Commissioner 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 S$1m.

37 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commissioner considered the following factors:

(a) the Organisation had initiated the data breach notification to the Commission and was co-operative in the investigations;

(b) the Organisation took prompt action (described in [12] and [13] above) to mitigate the impact of the data breach and to prevent future breaches of a similar nature from occurring;

(c) the extent of the unauthorised disclosure was limited, and the disclosure was only to a single third party, Tokyu Hands (which has confirmed that it has destroyed or returned the renewal notices received). While the exact number of affected individuals cannot be determined and there remains a possibility that individuals continue to be affected, the Commissioner is satisfied that the Organisation has taken steps to minimise the impact on any affected individual.

38 In consideration of the factors above and the circumstances of the present case, pursuant to s 29(2) of the PDPA, the Commissioner hereby directs that the Organisation pay a financial penalty of S$9,000 within 30 days of the Commissioner's direction, failing which, interest at the rate

6 [2018] PDP Digest 281.

specified in the Rules of Court[7] in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

7 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Habitat for Humanity Singapore Ltd

[2019] PDP Digest 200

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1707-B0971
Decision Citation: [2019] PDP Digest 200; [2018] SGPDPC 9

Openness Obligation *– Requirement to develop and implement policies and practices and communicate these policies and practices to staff*
Personal data *– Unnecessary disclosure of NRIC numbers – Stronger controls needed to protect sensitive personal data*
Protection Obligation *– Disclosure of personal data – Insufficient administrative security arrangements*

3 May 2018

BACKGROUND

1 On 20 July 2017, the Organisation sent out an e-mail to 32 of its volunteers with a PDF attachment comprising a batch of community involvement programme ("CIP") letters (the "CIP Letters") acknowledging the participation of each volunteer at an event organised by the Organisation (the "Incident"). The Personal Data Protection Commission (the "PDPC") was informed of the Incident on 22 July 2017 and commenced its investigations thereafter. I set out below my findings and grounds of decision based on the investigations carried out in this matter.

MATERIAL FACTS

2 The Organisation is a registered charity under the National Council of Social Services, which objectives include seeking to eliminate poverty housing worldwide by providing decent and affordable housing. In furtherance of its objectives, the Organisation organises community involvement programmes, where volunteers can participate in activities such

as mass clean-up events. After such events, the Organisation would generally send out a CIP letter to acknowledge and verify each individual volunteer's participation.

3 The Incident involved the disclosure of a batch of CIP Letters in an e-mail (the "E-mail") that was prepared by a manager (the "Manager") in the Organisation. The CIP Letters were created using the mail merge function in Microsoft Word which would fill in a CIP letter template with the names and NRIC numbers of the volunteers. This created a single Microsoft Word document containing the CIP Letters for all the volunteers, which the Manager then converted from Microsoft Word to PDF format. The Manager then sent the PDF containing the entire batch of CIP Letters to another member of staff ("Admin Staff"), along with the volunteers' e-mail addresses and instructed the Admin Staff to send out the CIP Letters.

4 The Organisation's usual practice was for the document containing the entire batch of CIP Letters to be segregated and split into individual CIP Letters before each CIP Letter was individually sent to its respective volunteers. However, in this case, neither the Manager nor the Admin Staff had prepared and/or handled any CIP Letters prior to the Incident. The Manager failed to instruct the Admin Staff on the proper procedure.

5 On 20 July 2017, the Admin Staff sent a mass e-mail to all the volunteers who were involved in the mass clean-up event, attaching the PDF document which contained the entire batch of CIP Letters. As a result, the PDF attachment containing the CIP Letters revealed the names and NRIC numbers of all the volunteers who had participated in the Organisation's mass clean-up event. Additionally, the E-mail was also sent with the e-mail addresses of all the recipients in the "cc" field. Consequently, the Organisation received two e-mails from the volunteers who had received the E-mail, expressing their concern that their personal data had been disclosed to other parties without their consent.

FINDINGS AND BASIS FOR DETERMINATION

6 The issues for determination are:

(a) whether the Organisation complied with its obligations under s 12 of the Personal Data Protection Act 2012[1] ("PDPA"); and

(b) whether the Organisation was in breach of s 24 of the PDPA.

7 As a preliminary point, the names, NRIC numbers and e-mail addresses disclosed in the E-mail and CIP Letters fall within the definition of "personal data" under s 2(1) of the PDPA, as it was clearly possible to identify an individual from that data.

8 Pursuant to s 53(1) of the PDPA, any act done or conduct engaged in by a person 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 by him, regardless of whether it was done or engaged in with the employer's knowledge or approval. The Organisation is therefore responsible for its employees' conduct in relation to the Incident.

Whether the Organisation complied with its obligations under section 12 of the Personal Data Protection Act

9 Section 12(*a*) of the PDPA requires an organisation to develop and implement policies and practices that are necessary to meet its obligations under the PDPA. Section 12(*c*) of the PDPA also requires the organisation to communicate to its staff information about such policies and practices.

10 The Organisation claimed to have instructed its employees on the Organisation's obligations under the PDPA and the importance of safeguarding its volunteers and donors' personal data. Employees who were required to deal with personal data were also briefed on the following data protection practices and procedures "on a need basis":

(a) to use the "bcc" function when sending out mass e-mails;

(b) to send the CIP Letters individually;

(c) to avoid sharing collected personal data with unauthorised third parties;

(d) to contact individuals only for purposes that they have given consent;

---

1 Act 26 of 2012.

(e) to use personal data only for the purposes for which it was collected; and

(f) to secure all documents containing personal data safely.

11 However, there were no documented policies, practices or procedures in relation to sending out the CIP Letters. Indeed, the Incident could very well have been averted if the Organisation had implemented, and documented, a standard operating procedure for the sending out of the CIP Letters. By the Organisation's own admission, the Manager had omitted to instruct the Admin Staff on the Organisation's usual procedure for sending out the CIP Letters and she "should have written down the instruction clearly for [the Admin Staff], which [she] had forgotten to do".

12 I take this opportunity to reiterate the benefits and importance of documenting an organisation's data protection policies and practices in a written policy as emphasised in *Re Furnituremart.sg*[2] ("*Furnituremart.sg*") at [14]:

> The lack of a written policy is a big drawback to the protection of personal data. Without having a policy in writing, employees and staff would not have a reference for the Organisation's policies and practices which they are to follow in order to protect personal data. Such policies and practices would be ineffective if passed on by word of mouth, and indeed, the Organisation may run the risk of the policies and practices being passed on incorrectly. Having a written policy is conducive to the conduct of internal training, which is a necessary component of an internal data protection programme.

13 In this regard, the Organisation was unable to demonstrate or produce any evidence that it had developed and implemented policies and practices necessary for it to comply with its obligations under the PDPA in respect of sending out the CIP Letters.

14 In addition, the Organisation did not provide any formalised data protection training for its employees. As the Commissioner observed in *Re National University of Singapore*,[3] data protection training may fall under both the openness obligation (specifically, s 12 of the PDPA) and the protection obligation (s 24 of the PDPA). Data protection training is an effective mode of communication of the Organisation's policies and practices to fulfil the openness obligation (s 12(*c*) of the PDPA).

---

2 [2018] PDP Digest 175.

3 [2018] PDP Digest 155 at [21].

15 The Manager's failure to communicate the Organisation's data protection policy was evidenced by the Admin Staff's lack of awareness of the use of the "bcc" function and the implications of her actions in respect of the E-mail. Although the Admin Staff claimed to have been instructed on the "rules with regard to volunteers' personal details", the fact that she: (a) did not query whether it was appropriate to send the entire batch of CIP Letters containing personal data to all the volunteers; and (b) did not think to check whether the e-mail addresses of the recipients of a mass e-mail should be inserted in the "bcc" field instead of the "to" or "cc" fields suggests that there was a lack of awareness of the Organisation's obligations under the PDPA.

16 Accordingly, I find that the Organisation has breached its openness obligation, given that it did not develop and implement a data protection policy as necessary for the Organisation to meet its obligations under the PDPA at the time of the Incident, and it did not communicate its data protection policies and practices to its staff, as required under ss 12(*a*) and 12(*c*) of the PDPA.

(b) Whether the Organisation was in breach of section 24 of the Personal Data Protection Act

17 Section 24 of the PDPA requires an organisation to protect the 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 In this case, the Organisation's informal practices and verbal reminders "on a need basis" were an insufficient security arrangement for the purposes of compliance with s 24 of the PDPA. The Organisation did not implement any checks and controls to prevent or minimise the risk of unauthorised disclosure of personal data. Knowing that the output produced by the Microsoft Word mail merge function was a single file containing the CIP Letters for all volunteers in the batch, the Organisation did not implement technical arrangements such as installing IT tools[4] that

4 There were IT tools reasonably available that would have enabled the community involvement programme letters to be generated from a template as separate documents. For instance, the installable PDF Split & Merge program

(*continued on next page*)

would have enabled the CIP Letters to be generated from the CIP letter template as separate documents. At the minimum, greater awareness of the need to protect the personal data of volunteers would have prompted the Admin Staff to process the PDF or Microsoft Word document containing the entire batch of CIP Letter manually in order to split the document into individual PDF files. The Manager would also have had a role to play in ensuring that this was done and could have implemented simple process checks to identify errors. Furthermore, technical controls could also have been installed to remind employees to use the "bcc" function when multiple e-mail addresses are pasted in the "to" or "cc" field.

Unnecessary disclosure of NRIC numbers

19 At this juncture, I observe that the disclosure of the volunteers' NRIC numbers in the CIP Letters was unnecessary as the CIP Letters had already referred to the volunteers by their full names. Given that an individual's NRIC number is a permanent and irreplaceable identifier which can be used to unlock large amounts of information relating to the individual, organisations should not disclose an individual's NRIC number except where it is required under the law or where it is necessary to accurately establish and verify the identity of the individual by way of the same. It is not apparent to me that the need to identify an individual in a CIP Letter was to such a degree of specificity that his or her NRIC number had to be included. The nature and function of a CIP Letter did not necessitate the publication of the volunteer's NRIC number.

20 Organisations that choose to disclose more sensitive data than is required for their business or legal purposes have to be able to defend such decisions and bear the burden of ensuring an appropriate level of security for the personal data of varying levels of sensitivity. As observed in *Re Aviva Ltd*[5] at [18]:

> The *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* states that an organisation should 'implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels

---

allows a single PDF or Microsoft Word output from a mail merge operation to be processed into individual PDF files.

5 [2018] PDP Digest 245.

of sensitivity'. *This means that a higher standard of protection is required for more sensitive personal data.* [emphasis added]

21 In the premises, I find that the Organisation failed to make reasonable security arrangements to protect the personal data in its possession and control, as the Organisation:

(a) did not put in place basic administrative security arrangements such as setting out its data protection policies and procedures in writing;
(b) did not implement any checks and controls to ensure that its employees were complying with its data protection practices and policies;
(c) did not provide any formalised data protection training for its employees;
(d) failed to properly supervise the employees who were in charge of preparing and sending out the CIP Letters; and
(e) did not have any other form of security arrangement to protect its volunteers' personal data.

DIRECTIONS

22 Having found that the Organisation is in breach of ss 12(*a*), 12(*c*), and 24 of the PDPA, I am empowered under s 29 of the PDPA to give the Organisation such directions as I deem fit to ensure compliance with the PDPA.

23 In assessing the breach and determining the directions to be imposed, I took into account, as an aggravating factor, the fact that the personal data disclosed included the volunteers' NRIC numbers, which were of a sensitive nature.

24 I also took into account the following mitigating factors:

(a) the disclosure only affected a limited number of people; and
(b) the Organisation had co-operated fully in the PDPC's investigation.

25 Pertinently, the PDPC has recently issued a public consultation on the proposed advisory guidelines for NRIC numbers, which, *inter alia*, discourages the indiscriminate use of NRIC numbers. Due weight has been given to the unsatisfactory practices that currently abound. Our practices as

a society need to be improved as we become more knowledgeable about the risks of identity theft and other identity-related risks (and I do not restrict this caution as referring only to online risks). In future, similar conduct may call for the imposition of a financial penalty as proposed changes to the advisory guidelines on the collection, use and disclosure of NRIC numbers are implemented. This case should serve as a clarion call for all organisations to start handling personal data such as NRIC numbers, which are unique and permanent identifiers of individuals, with a much higher degree of care and discernment than the present.

26 I hereby issue the following directions to the Organisation:

(a) to conduct a review of all its activities involving the handling of personal data of its volunteers and donors;

(b) to put in place a data protection policy, including process safeguards and written internal policies, such as standard operating procedures, to comply with the provisions of the PDPA;

(c) to arrange for personal data protection training for its staff; and

(d) to complete the above directions within 90 days from the date of this decision and inform the Deputy Commissioner of the completion thereof within one week of implementation.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re NTUC Income Insurance Co-operative Ltd

[2019] PDP Digest 208

Coram: Tan Kiat How, Commissioner
Case Number: DP-1706-B0894
Decision Citation: [2019] PDP Digest 208; [2018] SGPDPC 10

Powers of investigation *– General duty of organisations to preserve evidence in investigation – Commissioner may draw adverse inference against organisation that destroys or deletes relevant documents and records*
Powers of investigation *– Obligation to retain records relating to investigation after investigation has been completed pursuant to section 50(4) Personal Data Protection Act 2012 (Act 26 of 2012)*
Protection Obligation *– Disclosure of personal data – Insufficient administrative security arrangements*

3 May 2018

BACKGROUND

1 This matter deals with a flaw in the design of the Organisation's processes surrounding the printing of various types of letters resulting in the unauthorised disclosure of personal data of 214 of the Organisation's clients (the "Impacted Clients").

MATERIAL FACTS

2 The Organisation is an insurance co-operative that offers various types of insurance plans to its policyholders.

3 On 21 June 2017, a customer (the "Complainant") of the Organisation lodged a complaint (the "Complaint") with the Personal Data Protection Commission ("PDPC") alleging that she received a duplex printed letter from the Organisation correctly addressed to her, but the reverse of which was a letter addressed to another client of the Organisation. Subsequently, on 30 June 2017, the Organisation submitted a voluntary

notification of a breach of the Personal Data Protection Act 2012[1] (the "PDPA") which confirmed the Complainant's allegations and provided details surrounding the Complaint.

4 On 5 June 2017, the Organisation printed a batch of 426 letters that were sent out to its clients. These letters were no more than a page long. The vast majority of the 426 letters (the "Policy Letters") that the Organisation printed were letters reminding its clients to pay their insurance premium ("Premium Reminder Letters"). This batch of letters also included six letters ("Policy Cancellation Letters") informing the relevant clients of the termination of their insurance policies with the Organisation, and 32 letters recording the relevant clients' non-acceptance of the Organisation's offer of insurance coverage ("Non-Take Up Letters"). The personal data ("Personal Data") found in these letters are set out in the table below:

Policy Cancellation Letters	**Non-Take Up Letters**	**Premium Reminder Letters**
Name; Full residential address; Type of policy; Policy number; and Endorsement number.	Name; Full residential address; and Type of policy.	Name; Full residential address; Type of policy; Policy number; and Premium amount.

5 The Organisation was informed by some of its clients that, similar to the Complainant, they had each received a Policy Letter addressed to them the reverse of which was a letter addressed to another client (the "Incident").

6 An investigation was carried out under s 50(1) of the PDPA in relation to a breach of s 24 of the PDPA.

The Organisation's process for printing the Policy Letters

7 The Organisation's process for printing the Policy Letters was largely automated. Policy Letters issued by the Organisation to be mailed to its clients would be sent to the system (the "Printing System") used by the Organisation's print room operators. The computer files containing these

1 Act 26 of 2012.

Policy Letters were programmed, before the files were sent to the Printing System, to be printed either in simplex (*ie*, printed on a single side of the paper) or duplex (*ie*, printed on both sides of the paper) according to the type of letters to be printed. The print room operators would initiate the printing of the Policy Letters by releasing the files in the print queue.

8 On 5 June 2017, according to the Organisation one of the three printers in the print room was "overloaded". The Organisation uses the term "overloading" to describe the situation when too many files were automatically sent to one of the printers in the print room. This was a fairly common occurrence and there was a procedure to handle this overloading. The print room operator on duty would have to manually transfer the print files from one printer to another to ensure that the printing load was spread evenly across the three printers. The procedure for the manual transfer of print jobs was as follows:

(a) The print room operator was required to select the specific file to be transferred.

(b) The print room operator would then select the file name and choose the option "forward". A dialog box stating "enable queues" will appear.

(c) The print room operator would then select the particular printer available to receive the file for printing and type in "(dept)_simplex" or "(dept)_duplex" under "queue name" in the dialog box.

9 As a matter of protocol, the print room operator is required to choose to print the file in the format it was originally sent to the Printing System when he undertakes the manual transfer of the print job from one printer to another. In other words, if a letter sent to the Printing System was to be printed in simplex format, then the print room operator should choose to print the letter in simplex.

10 However, on this occasion the print room operator had mistakenly chosen to print the letters in duplex instead of simplex format. This led to two different Policy Letters addressed to two different policyholders being printed on each sheet of paper that was printed during the print run.

FINDINGS AND ASSESSMENT

Issue for determination

11 The issue to be determined is whether the Organisation had, pursuant to s 24 of the PDPA, put in place reasonable security arrangements to protect the Personal Data from unauthorised disclosure.

12 Section 24 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.

Whether the Organisation was in breach of section 24 of the Personal Data Protection Act

The Personal Data was disclosed without authorisation

13 It is not disputed that the Personal Data fell within the definition of "personal data" under s 2 of the PDPA as it was possible to identify the Impacted Clients from that information alone. It is also not in dispute that the Personal Data was disclosed mistakenly and without authorisation.

14 Based on the investigations carried out, the Commissioner found that the unauthorised disclosure of the Personal Data was a result of a breach of the Organisation's obligation to make reasonable security arrangements for the protection of the Personal Data. The reasons for this finding are set out below.

The Organisation did not implement any measures to prevent the Incident

15 According to the Organisation, the print room operator was required to conduct a visual check ("visual check") of 10% of printed letters for the quality of print and alignment. The print room operator was also required to reconcile (the "Reconciliation") the number of letters printed as shown on the electronic counter of the individual printers with the number of letters sent for printing as displayed on the Printing System. The quantity of the printouts would be recorded in a printout log book (the "Log Book"). No other checks or security arrangements were implemented

with respect to the printing process to prevent the unauthorised disclosure of personal data.

16 The Commissioner was of the view that the visual check and Reconciliation were not designed to adequately address the protection of personal data.

17 Such checks were to be undertaken by the same print room operator who printed the letters. As has been traversed in other cases, it is not advisable for an organisation to rely on a member of its staff checking his own work to ensure that he has undertaken a task properly to meet the Organisation's protection obligation under s 24 of the PDPA: see *Re Aviva Ltd*[2] at [28]; *Re Furnituremart.sg*[3] at [20]–[21].

18 Further, these checks had little to do with protecting personal data. The visual check was a check to ensure that the print on the letters was legible and not faded or smudged and that the letter was correctly aligned such that words were not missing or cut off. The Organisation did not require the print room operator or any other staff to check that the information on both sides of duplex printed letters was meant for the same individual. There was also no requirement to check that Policy Letters were printed in the correct format, either simplex or duplex, as it was originally sent to the Printing System when a manual transfer of print jobs was undertaken.

19 The Reconciliation check would not catch an error in the choice of print format as the reconciliation was based on the number of letters which were sent to be printed against the number of pages printed as shown on the electronic counter of the printers. The number of pages printed would not change whether or not the letters were printed in the simplex or duplex format, it would merely show the number of pages printed in total. If five letters sent to the Printing System were printed, the electronic counter on the printer would show that five pages were printed, whether or not the letters were printed in the simplex or duplex format.

20 While investigations showed that a check was implemented at the enveloping stage, this check also did not address situations such as this Incident. At the enveloping stage, letters would be inserted into a mail

2 [2018] PDP Digest 245.

3 [2018] PDP Digest 175.

insertion machine for enveloping by one of the Organisation's mail insertion operators. The mail insertion operator was required to reconcile the number of sealed envelopes with the number of sheets of paper printed by the print room operator. If instead, the mail insertion operator was required to reconcile the number of sealed envelopes with the number of letters sent for printing, the Incident would likely have been prevented. As it stands, however, this final check also did not address situations such as this Incident.

21 Given that the Personal Data includes insurance data of the Complainant and other policyholders, the Commissioner would also highlight that information such as the type of insurance policy and insurance premium amounts has been determined in the past to be sensitive personal data: *Re Aviva Ltd*[4] at [38(b)]. The Commissioner has in the past expressly stated his view that an Organisation should accord a higher standard of protection to sensitive personal data: *Re Aviva Ltd*[5] at [18]–[19]. In this case, the standard of protection provided was not even sufficient for non-sensitive personal data.

22 In the circumstances, taking the printing and enveloping process as a whole, the Commissioner finds that the Organisation did not implement reasonable security arrangements to prevent the unauthorised disclosure of the Personal Data.

Organisations are required to preserve documents and records relating to an investigation

23 Before moving on to the remediation action taken by the Organisation and to the directions in this matter, the Commissioner takes this opportunity to remind the Organisation and organisations in general about their duty to preserve evidence, including but not limited to documents and records, in relation to an investigation by the PDPC.

24 This issue arises in this case because the Organisation was unable to provide copies of the Log Book when asked pursuant to the investigation powers set out in the Ninth Schedule of the PDPA; the Organisation alleged that the copies were destroyed, in line with the Organisation's three-

4 [2017] PDP Digest 107.

5 [2018] PDP Digest 245.

month retention period for such records. Notably, the destruction of copies of the Log Book took place *after* the commencement of investigations.

25 The Commissioner does not look favourably on the destruction or deletion of potentially relevant documents and records and may impose tough sanctions on any organisation that is found to have destroyed or deleted such documents or records.

26 Analogous to the preservation of evidence in civil proceedings, the Commissioner will consider, in deciding on the necessary and appropriate sanctions to be imposed, amongst other things, whether the deletion or destruction of the documents or records was deliberate (which includes negligent or reckless conduct resulting in destruction) and to what extent the deletion or destruction of the records or documents prejudiced a fair investigation into a potential breach of the PDPA.[6] In summary, the approach of the Commission will be to first consider whether a fair investigation into a potential breach of the PDPA is possible. If investigations may still proceed, particularly in reliance on evidence that may still substantially be obtained from other sources, the Commission may draw adverse inferences against the organisation that failed to preserve and produce any piece of evidence to the effect that had the evidence been produced, it would have been adverse to its case.[7] Adverse inferences may also be drawn against a complainant if the evidence ought to have been preserved and produced by the complainant.

27 Another pertinent factor for consideration is whether the litigation or legal proceedings was anticipated or contemplated by the party that destroyed the document or record. In the case of *K Solutions Pte Ltd v National University of Singapore*[8] ("*K Solutions*") the appellant had anticipated litigation for some time before its action was filed and had given instructions to its staff to back up the e-mail in their accounts. The High

---

6 *K Solutions Pte Ltd v National University of Singapore* [2009] 4 SLR(R) 254 at [125].

7 See s 116 of the Evidence Act (Cap 97, 1997 Rev Ed), which states: "The court may presume the existence of any fact which it thinks likely to have happened, regard being had to the common course of natural events, human conduct, and public and private business, in their relation to the facts of the particular case."

8 [2009] 4 SLR(R) 254.

Court did not find it credible that all of the appellant's internal e-mails had been deleted without backup, and determined that the appellant had deliberately suppressed documents and had lied about it.[9] In contrast, the court in *Tan Chor Chuan v Tan Yeow Hiang Kenneth*[10] dismissed the plaintiff's application for striking out as it did not find anything sinister in the defendants' explanation for the deletion of the e-mail in question – it was the defendants' practice to delete e-mails from their computer systems regularly to free up memory space; the defendants saw no necessity to archive or keep copies of e-mails after the EGM; and litigation had not been anticipated at the time. The court determined that the deletion of the e-mail was not an attempt to pervert the course of justice.[11] In *K Solutions*, the court exercised its discretion to dismiss the case brought by the party in default. Applying the same principles to investigations conducted by the PDPC, the Commissioner may discontinue or refuse to conduct investigations under s 50(3)(*e*) of the PDPA.

28 The obligation to preserve evidence is taken further by s 50(4) of the PDPA, which imposes an obligation on organisations to retain records relating to an investigation, for one year or such longer period as directed, after the investigation has been completed. This ensures that evidence relevant to any possible application for reconsideration or appeal from an investigation remains available even after investigations are completed.

29 Given the foregoing, the Commissioner takes the view that organisations should have a detailed litigation hold policy in place to ensure that documents and records relating to an investigation or potential investigation of a breach of its obligations under the PDPA are preserved and not deleted, disposed of or destroyed. Organisations should also ensure that relevant procedures and practices are fully implemented to give effect to such a litigation hold policy.

30 In respect of the matter at hand, however, the Commissioner is of the view that the contents of the Log Book, which was meant to have recorded the Reconciliation check by the print room operator, were not required for the Commissioner to make a finding of breach of s 24 given the finding

9 *K Solutions Pte Ltd v National University of Singapore* [2009] 4 SLR(R) 254 at [131]–[137].

10 [2004] SGHC 259.

11 *Tan Chor Chuan v Tan Yeow Hiang Kenneth* [2004] SGHC 259 at [24]–[25].

that the Reconciliation was not a security arrangement designed to prevent the Incident. As such, the Commissioner did not impose any sanctions against the Organisation for the failure to preserve copies of the relevant Log Book.

REMEDIATION ACTIONS TAKEN BY THE ORGANISATION

31 The Commissioner notes that after the data breach incident, the Organisation undertook the following remediation actions:

(a) The manual transfer of print jobs may now only be activated by the supervisors of the print room operators. Once activated, the print room operators may undertake the manual transfer of print jobs under the oversight of the supervisors.

(b) Both the print room operators and mail insertion operators are now required to check that the letters are printed in the correct format (*ie*, either in the simplex or duplex formats) by comparing the files sent for printing in the Printing System with the printed letters before enveloping. The checks will be done on 20% of letters printed in a batch on a random basis where no manual transfer of print jobs is undertaken. Where a manual transfer is undertaken, the print room operator and the mail insertion operator are required to check all letters.

(c) The above measures have been included in the Standard Operating Procedure ("SOP") for the print and mail room operations. A briefing was also held for the print and mail room operators to inform them of the changes in the SOP.

DIRECTIONS

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

33 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commissioner took into account the following aggravating and mitigating factors:

Aggravating factors

(a) the unauthorised disclosure was systemic in nature;

(b) the Personal Data included sensitive personal data. However, in this regard, the Commissioner took cognisance that the insurance data that was disclosed in this matter was less sensitive than personal data of the type disclosed in *Re Aviva Ltd*[12] which included the names of beneficiaries and dependents and the sum insured;

Mitigating factors

(c) the Organisation had co-operated fully with investigations;

(d) the Organisation took prompt action to remedy the flaw in the process; and

(e) there was no evidence to suggest that there had been any actual loss or damage resulting from the unauthorised disclosure.

34 Pursuant to s 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that the Organisation did not make reasonable security arrangements to protect the Personal Data and is in breach of s 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$10,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

12 [2017] PDP Digest 107.

Grounds of Decision

Re Information Technology Management Association (Singapore)

[2019] PDP Digest 218

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1708-B1019
Decision Citation: [2019] PDP Digest 218; [2018] SGPDPC 11

Openness Obligation *– Requirement to develop and implement policies and practices*
Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

14 May 2018

BACKGROUND

1 On 10 August 2017, the Organisation informed the Personal Data Protection Commission ("Commission") of its inadvertent disclosure of personal data. The facts disclose a straightforward breach of s 24 of the Personal Data Protection Act 2012[1] ("PDPA").

2 The Organisation engaged a travel service provider to organise a study trip for 49 delegates. On 8 August 2017, the Organisation received an e-mail with two attachments from the travel service provider. One attachment was a list containing full names, gender, nationality, dates of birth and passport numbers of 28 delegates (the "List").

3 The Organisation forwarded the e-mail to the 49 delegates on 10 August 2017. The List was inadvertently included in the e-mail. This resulted in the inadvertent disclosure of the personal data in the List.

4 One delegate provided feedback to the Organisation on the List. Upon notification of the error, the Organisation promptly e-mailed an

1 Act 26 of 2012.

apology to the 28 delegates. It subsequently contacted all 49 recipients and requested that they delete the copy of the List that they had received.

5 The issues to be determined in this case are:

(a) whether the Organisation breached s 24 of the PDPA to protect the personal data in the List; and

(b) whether the Organisation breached s 12(*a*) of the PDPA to develop and implement policies and practices to comply with the Act.

DID THE ORGANISATION BREACH SECTION 24?

6 An organisation must protect personal data in its possession or under its control under s 24 of the PDPA ("Protection Obligation"). In this regard, it must take reasonable steps to prevent unauthorised access, copying, modification, or disposal personal data.

7 The Organisation's core business was running a membership programme. Its functions involved frequent sending of e-mails including personal data. The Commissioner's *Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data* (published on 20 January 2017) states that employees should ensure that attachments are checked and verified that they are for the intended recipients. In this case, the Organisation had failed to do so when sending the e-mail containing the List to all 49 recipients. The result was the personal data in the List being disclosed to delegates who were not intended to receive such data of other delegates. The Organisation was therefore found in breach of s 24 of the PDPA.

DID THE ORGANISATION BREACH SECTION 12(*a*)?

8 Section 12(*a*) required the Organisation to develop and implement policies and practices to comply with the PDPA.

9 The Organisation had a Personal Data Protection Statement ("PDP Statement"). It outlined how collected personal data might be used. It also stated that access to personal data was limited to employees who needed to process it. Likewise, personal data would be shared on a need-to-know basis. For external communications, personal data would be shared only when there was a "legitimate reason". An employee was assigned to process

all personal data handled by the Organisation. The employee had previously attended formal training on the requirements of the PDPA and had been briefed on the Organisation's protection of personal data.

10 It was assessed that the Organisation's PDP Statement complied with the requirement under s 12(*a*) to develop policies to meet its obligations under the PDPA. Its attempt to limit access to personal data to the employee who had been given PDPA compliance training was assessed to comply with the requirement to implement the policies in its PDP Statement. Finally, the Organisation's efforts to implement its personal data protection polices under s 12(*a*) were taken as forms of practices on the ground to help employees manage the risk of unauthorised disclosure of or access to personal data through e-mails and other external communications.

11 Accordingly, the Organisation was not found in breach of s 12(*a*) of the PDPA.

REMEDIAL MEASURES TAKEN

12 Following the incident, the Organisation required employees to review all e-mails and attachments before sending or forwarding. They are also required to check whether personal data is being sent to unintended and/or unauthorised recipients.

13 In assessing this case, I took into account the following:

(a) the Organisation's prompt action to inform all 49 delegates to delete the List;
(b) the Organisation's voluntary notification of the incident and co-operation in the investigation; and
(c) the Organisation's remedial measures assessed to be reasonable to address risk of similar incidents.

14 In view of the factors noted above, I decided to issue a warning to the Organisation for the breach of its obligation under s 24 of the PDPA as neither further directions nor a financial penalty is warranted in this case.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Watami Food Service Singapore Pte Ltd

[2019] PDP Digest 221

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1711-B1312
Decision Citation: [2019] PDP Digest 221; [2018] SGPDPC 12

Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

14 May 2018

BACKGROUND

1 Watami Food Service Singapore Pte Ltd (the "Organisation") is in the restaurant business. On 10 November 2017, information was received the Organisation's internal Staff Code Name List (the "List") was accessible via its website. The List contained personal data of 405 employees of the Organisation, namely their full names and staff codes.

2 The List was to facilitate the entry of new employee staff codes into the Organisation's point-of-sale system. This information is not current as it was dated between 2009 and 2013. The List was meant for internal use within the Organisation.

3 The Organisation did not know when or why the List was uploaded to the Organisation's website server. As there was no restriction on access, the List was indexed by search engines and made publicly searchable online. The URL containing the List was subsequently removed by Fairwin International Limited ("Fairwin"), a vendor the Organisation engaged to maintain its website.

4 The Organisation was in possession and/or control of the personal data in the List. Section 24 of the Personal Data Protection Act 2012[1] ("PDPA") required the Organisation to protect the personal data in the List. This included protection against risk of unauthorised access.

5 I rely on the common law concept of *res ipsa loquitur* in this case as the Organisation is unable to explain how the List which it maintained for internal use was uploaded to its website. The Organisation also did not exercise reasonable control of the information on its website, since it was not aware that the List has been accessible on its website and searchable via online search engines.

6 Neither did it adopt reasonable steps to monitor against information leak on its website. The period that the List was thus exposed could possibly have commenced from 2013, but could also have been a shorter period. The Organisation's poor oversight and control did not enable it to establish the period of exposure. As a result, the personal data of its staff remained on its website undetected until being contacted by the Personal Data Protection Commission. Exercising better oversight of its website content could have led to an earlier discovery and removal of the URL giving access to the List.

7 In the course of investigations, it was further discovered that the Organisation failed to train its staff to protect the personal data in its possession or control. The Organisation's privacy policy included proper personal information management. However, its staff were not trained in protecting personal data other than occasional reminders, for example to use alphanumeric passwords. No formal instructions were given to the staff on the Organisation's data protection policies or other forms of data protection training.

8 Accordingly, I find that the Organisation did not put in place reasonable security arrangements to protect personal data in its possession or control against risk of unauthorised access. The Organisation is therefore in breach of s 24 of the PDPA.

---

1 Act 26 of 2012. Section 24 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.

9 In assessing the breach and determining the directions to be imposed on the Organisation, I took into account the following:

(a) the Organisation's prompt instruction to Fairwin to delete the URL on its website;
(b) the Organisation's co-operation in the investigation; and
(c) its remedial measures, where the Organisation restricted access to the website server to only one person, and also reminded all staff that all documents containing sensitive personal data should be password-protected and not be uploaded online.

10 In view of the factors noted above, I have decided to issue a warning to the Organisation for the breach of its obligation under s 24 of the PDPA as neither further direction nor a financial penalty is warranted in this case.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re MyRepublic Limited

[2019] PDP Digest 224

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1701-B0463
Decision Citation: [2019] PDP Digest 224; [2018] SGPDPC 13

Consent Obligation *– Use of personal data for debt management purposes*

14 May 2018

BACKGROUND

1 The complaint concerns the use of a customer's personal data by MyRepublic Limited's (the "Organisation") appointed debt collection company, Apex Credit Management Pte Ltd ("Apex Credit"), for the purpose of debt recovery. The Organisation is a telecommunications company which provides fibre broadband services in Singapore.

2 The Complainant terminated his account with the Organisation on 25 September 2016. He claimed that he did not have any outstanding debt with the Organisation. However, he was subsequently contacted by Apex Credit on two occasions. The purpose was to pursue payment of outstanding amounts purportedly owed to the Organisation. First was via letter sent to the Complainant on 3 October 2016. Second was via a phone call on 10 October 2016. The Organisation disclosed that its systems had identified the Complainant's account for debt collection based on its debt aging status.

3 This case concerns s 13[1] of the Personal Data Protection Act 2012 ("PDPA"). In particular, the issues are:

---

1 Section 13 of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA") requires either that (a) the individual gives, or is deemed to have given, his consent to the collection, use or disclosure of his personal data; or
(*continued on next page*)

(a) whether consent was given by the Complainant for his personal data to be used for debt collection purposes; and

(b) whether it was reasonable for the Organisation to have deemed that the Complainant was in debt at the material time.

Whether consent was given by the Complainant for his personal data to be used for debt collection purposes?

4 When customers sign up for the Organisation's services, their consent was obtained for the use of their personal data for debt management purposes. This was accomplished through the Organisation's terms and conditions, which state:

> By having the Services we provide activated in your premises and/or by using them you are giving us your consent to use your personal information for … credit assessment, *debt management*, preventing fraud … [emphasis added]

5 The Complainant had therefore consented to his personal data to be used for debt management when he signed up for the Organisation's services.

Was it reasonable for the Organisation to deem that the Complainant was in debt at the material time?

6 The incident was caused by an administrative time lag in the Organisation's systems. Investigations disclosed the following: The bank GIRO deduction for the amount owed by the Complainant to the Organisation was successfully processed on 28 September 2016. The Organisation's aging report to identify "terminated" and "suspended" accounts with outstanding payments was updated for records up to 29 September 2016, 2359hrs. Although the bank GIRO deduction report was received by the Organisation on 29 September 2016, it was only updated on 30 September 2016. As a result, the Complainant's account was included in the aging report and sent to Apex Credit on 30 September 2016. Based on the aging report received, Apex Credit commenced debt collection efforts against the Complainant.

(b) collection, use or disclosure without consent is required or authorised under the PDPA or any other written law.

7 I am mindful that while the PDPA imposes data protection obligations on organisations, the Act does not demand infallibility in an organisation's personal data processing activities and systems. Rather, it requires organisations to do what is reasonable to fulfil their obligations. Batch processing of arrears status is commonly practised. In this case, administrative time lag was one day. Debt collection efforts took place within a short span of eight days and it immediately ceased once Apex Credit was informed by the Complainant that the outstanding payment had been settled.

8 I find that a weekly update of customers' account status to be a reasonable practice. I also note that the inconvenience to the Complainant was no more than a letter and phone call, both of which were private communications directed to him. Apart from annoyance and the displeasure of having to deal with requests to repay a debt that he had already settled, there was no embarrassment or harm caused. I am therefore of the view that the Organisation has not breached s 13 of the PDPA.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Credit Bureau (Singapore) Pte Ltd

[2019] PDP Digest 227

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1707-B0946
Decision Citation: [2019] PDP Digest 227; [2018] SGPDPC 14

Accuracy Obligation *– Requirement to ensure personal data disclosed to another organisation is accurate and complete*
Retention Limitation Obligation *– Reasonable to assume purpose for which personal data was collected is no longer served by retaining data and retention is no longer necessary for legal or business purposes*

14 May 2018

BACKGROUND

1 This complaint concerns the accuracy and retention of the Complainant's personal data by Credit Bureau (Singapore) Pte Ltd ("the Organisation"). The Organisation is a consumer credit bureau. It aggregates credit-related information from its participating members. The risk profiles of individuals are presented in its Enhanced Consumer Credit Report ("ECCR").

2 The complainant had a bankruptcy application taken out against him in June 2012. The bankruptcy application was withdrawn by the creditor in July 2012. The Complainant was given a "HX" risk grade in this ECCR. A "HX" risk grading meant that there could be a past or existing bankruptcy record associated with the Complainant. The Complainant felt that a "HX" risk grading was inaccurate as he thought that it implied that he had an outstanding bankruptcy record or was not creditworthy. He therefore requested the Organisation to amend his risk grading.

3 The Organisation informed the Complainant that it was its practice to display bankruptcy-related data for five years. The Complainant then lodged a complaint against the Organisation to the Personal Data

Protection Commission on 24 May 2017. The complaint was that the Organisation had retained his personal data when it was no longer necessary for legal or business purposes.

FINDINGS AND BASIS FOR DETERMINATION

4 This case concerns the accuracy and retention obligations under the Personal Data Protection Act 2012[1] ("PDPA"), with respect to the bankruptcy information in the ECCR. In particular, the issues are:

(a) whether the Organisation had made a reasonable effort to ensure that the personal data it had collected was accurate and complete pursuant to s 23(*b*); and

(b) whether the Organisation had retained the Complainant's personal data when it was no longer necessary for legal or business purposes pursuant to s 25 of the PDPA.

*Did the Organisation breach section 23(*b*) of the Personal Data Protection Act?*

5 Section 23(*b*) of the PDPA requires an organisation to make a reasonable effort to ensure that the personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be disclosed by the organisation to another organisation.

6 In this case, the Organisation had explained that a "HX" rating merely meant that there was a past or existing bankruptcy record associated with the individual concerned. A "HX" rating did not represent that the individual was a bankrupt. The Organisation had also cautioned creditors against upfront rejection of credit applications of applicants with "HX" ratings. This buttresses the Organisation's position that the "HX" rating alone does not determine creditworthiness.

7 According to the Association of Banks in Singapore ("ABS"), financial institutions ("FIs") consider information from several sources when making lending decisions. Apart from searches with credit bureaux, FIs also conduct public registry searches.[2] Records from the Insolvency & Public Trustee

1 Act 26 of 2012.

2 Including publicly available litigation and bankruptcy information.

Office ("IPTO") also showed that he was not a bankrupt. FIs would have been able to obtain the same information on the Complainant when conducting their own due diligence. Generally, FIs' creditworthiness assessment varies according to their risk appetite, internal assessment policies, portfolio delinquency and loss experience.

Did the Organisation breach section 25 of the Personal Data Protection Act?

8 Section 25 of the PDPA requires an organisation to cease retaining its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer served by retention of the personal data; and retention is no longer necessary for legal or business purposes.

9 The Organisation displays bankruptcy-related information for five years in its ECCR.[3] This aligns with the display period of the publicly available Insolvency Search maintained by the Insolvency & Public Trustee Office. The five-year retention policy gives FIs useful credit history of potential borrowers. Along with other information sources, this facilitates FIs' lending decisions.

10 I do not think that a five-year display period for bankruptcy-related information is unreasonable. The Organisation provides credit reporting services and the retention of bankruptcy-related information in order to deliver its services is a valid business purpose.

CONCLUSION

11 For the reasons set out above, I do not think that the Organisation has breached s 23(*b*) or s 25 of the PDPA.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

3 Including "HX" ratings.

Grounds of Decision

Re Spring College International Pte Ltd

[2019] PDP Digest 230

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1705-B0799
Decision Citation: [2019] PDP Digest 230; [2018] SGPDPC 15

Consent Obligation *– Disclosure of personal data on social media for marketing purposes without consent*
Consent Obligation *– Overly broad consent clause*
Notification Obligation *– Failure to notify students of purposes for disclosure*
Personal data *– Disclosure of personal data of minors*
Purpose Limitation Obligation *– Disclosure of personal data on social media for marketing purposes without notifying individual of purposes for such disclosure*

24 May 2018

BACKGROUND

1 This matter involves a private educational institution that posted information about its students, including their names and photographs, on a public social media page, in order to promote its courses. The Organisation operates a private educational institution, known as "Spring College International Pte Ltd" ("SCI"), that offers various academic courses to students of varying ages and levels. A complaint was made to the Personal Data Protection Commission ("PDPC") regarding the unauthorised disclosure of a student's personal data on the Organisation's Facebook page. The complaint was made by the student's parent ("the Complainant").

2 The Commissioner's findings and grounds of decision, based on the investigations carried out in this matter, are set out below.

MATERIAL FACTS

3 Since September 2010, the Organisation has maintained a Facebook page which is accessible to the general public, titled "Spring College International". In December 2015, the Complainant enrolled her son ("Individual A") as a student in SCI. Sometime thereafter, the Complainant came across a post on the Organisation's Facebook page, dated 24 April 2016 ("Post A"). The post contained the following text:

> Application for Supplementary Admissions Exercise for International Students
>
> 1 We are pleased to inform you that your application for admission to a secondary school through the Supplementary Admissions Exercise for International Students is successful. The results of your application are as follows:
>
> …

4 Post A further set out the following information about Individual A: full name; partially masked passport number; date of birth; application result for Supplementary Admissions Exercise for International Students ("AEIS"); primary school assigned to; level of study; and the length of Individual A's study period in SCI.

5 The Complainant subsequently discovered that Post A had been indexed by Google's search engine and would be publicly displayed as a search result on Google if Individual A's name was used as the search term. The summary on Google's search results page displayed part of the information contained in Post A, including Individual A's name, partially masked passport number and date of birth.

6 The Complainant informed the Organisation of her objection to the publication of her son's details on its Facebook page, following which the Organisation took down Post A and took steps to render Post A non-indexable by online search engines. The Complainant also submitted a complaint to PDPC, in which the Complainant alleged that the Organisation had not obtained consent to publish her son's personal data on its Facebook page.

7 In the course of the investigation, three other posts containing student data on the Organisation's Facebook page were uncovered, dated on or around 25 April 2016:

(a) **Post B**: data set of an individual student ("Individual B"), containing full name; partially masked FIN number; partially masked passport number; date of birth; photograph of Individual B standing under the Organisation's wall logos, next to another individual; application result for AEIS; primary school assigned to; level of study; and the length of Individual B's study period in SCI;

(b) **Post C**: data set of an individual student ("Individual C"), containing full name; partially masked FIN number (without passport number); date of birth; photograph of Individual C standing in between two other individuals, and under the Organisation's wall logos; application result for AEIS; primary school assigned to; level of study; and the length of Individual C's study period in SCI; and

(c) **Post D**: titled "Top students of the preparatory course for AEIS", containing information on multiple individual SCI students comprising full names; mugshots of these individuals; course duration; schools assigned to; and the level of study.

8 The Organisation did not dispute that the various Facebook posts contained the personal data of its students. The Organisation also did not deny responsibility for publishing the various Facebook posts. According to the Organisation, the various Facebook posts were made in order to share the activities and courses of SCI, for the purpose of creating brand awareness and attracting more students to register with SCI.

FINDINGS AND BASIS FOR DETERMINATION

9 The issues for determination are:

(a) whether the Organisation had complied with its obligation under s 13 of the Personal Data Protection Act 2012[1] ("PDPA") to obtain valid consent before disclosing the personal data of its students; and

(b) whether the Organisation had complied with its obligation under s 18 of the PDPA to only use and disclose personal data for purposes (i) that a reasonable person would consider

1 Act 26 of 2012.

appropriate in the circumstances; and (ii) that its students have been informed of.

The Consent and Notification Obligations

10 Under the PDPA, the concepts of notification of purpose and consent are closely intertwined. The PDPA adopts a consent-first regime. Unless an exception to consent applies, an individual's consent has to be sought: see s 13 of the PDPA, which imposes on an organisation the obligation to obtain the consent of an individual before collecting, using or disclosing that individual's personal data ("Consent Obligation"). Consent must, of course, be obtained from the individual with reference to the intended purpose of collection, use or disclosure of that individual's personal data; s 20 of the PDPA requires an organisation to notify an individual of such intended purpose ("Notification Obligation").

Personal data relating to minors

11 At this juncture, it is relevant to note that this case involved the personal data of minors. Individual A was nine years old at the time Post A was made; Individual B was eight years old at the time Post B was made; and Individual C was 11 years old at the time Post C was made. Post D contained the personal data of numerous individuals who were also minors at the time the post was made.

12 As discussed in the PDPC's *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* ("Selected Topics Guidelines"), certain considerations may arise when dealing with the personal data of minors.[2] In particular, where the personal data of a minor is involved, the issue of whether the minor is able to effectively give consent on his own behalf may arise. In this regard, organisations should take appropriate steps to ensure that the minor can effectively give consent on his own behalf, or if not, the organisation should obtain consent from an individual who is legally able to

2 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at paras 8.1–8.13.

provide consent on the minor's behalf, such as the minor's parent or guardian.[3]

13 As stated in the Selected Topics Guidelines:[4]

> 8.1 The PDPA does not specify the situations in which a minor (that is, an individual who is less than 21 years of age) may give consent for the purposes of the PDPA. In general, whether a minor can give such consent would depend on other legislation and the common law …
>
> …
>
> 8.3 For situations where there is no legislation that affects whether a minor may give consent, the issue would be governed by the common law. In this regard, the Commission notes that there is no international norm on when minors may exercise their own rights under data protection laws… some countries have enacted legislation to specifically protect minors below a certain age. *For example, in the United States, the Children's Online Privacy Protection Act ('COPPA') requires certain organisations to obtain verifiable parental consent to collect personal data from children under 13 years of age.*
>
> …
>
> 8.5 The Commission notes that the *age threshold of 13 years appears to be a significant one* in relation to according protection to minors …
>
> 8.6 The Commission is of the view that organisations should generally consider whether a minor has sufficient understanding of the nature and consequences of giving consent, in determining if he can effectively provide consent on his own behalf for purposes of the PDPA … *the Commission will adopt the practical rule of thumb that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf. However, where, for example, an organisation has reason to believe or it can be shown that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from an individual, such as the minor's parent or guardian, who is legally able to provide consent on the minor's behalf.*
> [emphasis added]

---

3 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at paras 8.7–8.9.

4 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at paras 8.1, 8.3, 8.5 and 8.6.

14 While there was no allegation in this case that the Organisation had purported to obtain consent from individuals who lacked sufficient legal capacity to give such consent, it is nevertheless worth highlighting that it would be prudent for organisations to take additional precautions and/or safeguards when collecting, using or disclosing the personal data of minors, bearing in mind that there is "generally greater sensitivity surrounding the treatment of minors".[5] There is no magic in the age of 13 as selected by the PDPC. The key determinant is whether the minor or young person is capable of understanding the nature and consequences of giving consent. The onus is on the organisation to determine whether consent may be obtained from a young person above the age of 13 or whether, despite being above 13 years of age, it is more prudent to obtain consent from the young person's parent or guardian. Restricting my analysis only to the circumstances of this case, I would have thought that the use of minors' personal data to publicise and market the Organisation's services is one of those purposes that an organisation ought to have conducted itself with a greater degree of prudence and should have sought consent from the young person's parent or guardian, even if the young person had been older than 13. I probably would have come to a different conclusion if, for example, the young person was participating in a school activity and a photograph had been taken during the event and used by the organisation in its regular newsletter, college annual or blog that reports on its activities and sporting achievements. In any event, the minors in this case were all below 13 years old and thus, even by the rule of thumb adopted in the Selected Topics Guidelines, consent ought to have been obtained from the minors' parents or guardians.

Whether the Organisation complied with its obligation to obtain consent for the disclosure of its students' personal data

15 In its responses to the PDPC, the Organisation stated that, when registering with SCI, students (or their parents, as the case may be) would be required to sign an enrolment form which contained a term stipulating that they would adhere to SCI's student handbook. The relevant term in the enrolment form is stated as follows:

---

5 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at para 8.12.

> By signing the form, I acknowledge that I was informed that the course is on-going. I confirm that all documents provided by me are true. I have received and will adhere to the student handbook issued by SCI.

16 Clause 15.1 of SCI's student handbook, entitled "Data Protection Notice & Consent", states:

> 15.1 The information provided in Application Form is to enable to SCI to:
>
> (a) Administering and/or managing the Applicant's application(s) for Admission and Enrolment;
>
> (b) Managing the Applicant's relationship with SCI
>
> (including the announcement of statements or notices of the Applicant, sending the Applicant marketing, advertising and promotional information, including materials and information on courses in SCI, general student-related activities within SCI, as well as related talks, seminars and/or events via postal mail, electronic mail, SMS or MMS, fax and/or voice calls; and);
>
> (c) Processing the Applicant's application(s) for scholarships and/or financial aid, and if successful, administering and/or managing the Applicant's scholarship and/or financial aid programmes, which may include use of personal data for direct marketing purposes for event invitations, surveys and/or publicity of SCI' financial aid programmes;
>
> (d) Responding to requests for information from public agencies, ministries, statutory boards or other similar authorities
>
> (e) Allow the compilation and analysis of statistics for marketing purpose
>
> [emphasis added]

17 Clauses 15.1(a) to 15.1(d) of the student handbook are concerned with matters that can best be described as administrative in nature. These clauses are not relevant to the disclosure of students' personal data on the Organisation's Facebook page in the present case.

18 In its responses to the PDPC, the Organisation sought to rely on clause 15.1(e) of its student handbook, in order to assert that it had obtained consent for the disclosure of its students' personal data in its various Facebook posts. However, I do not think that cl 15.1(e) of the student handbook adequately covers the disclosure of personal data in the various Facebook posts by the Organisation in this case. Clause 15.1(e) contains a general reference to the "compilation and analysis of statistics". The intent and purpose of statistical analysis is very different from the use in this case. Statistical analysis goes towards identifying how the Organisation may be more effective in delivering its services, in this case,

educational services. This is an acceptable use of personal data, whether in an anonymised form, aggregated (or compiled) or even in personally identifiable form (with consent or in reliance on the research exceptions in the PDPA). Organisations ought to, and are encouraged to do so, in order to understand their customers better and fine-tune their products or services to better cater to their customers' needs and preferences. Of course, one of the ends is to enable the organisation to design its marketing strategy more effectively. The point to note is that the use of the data is indirect and goes towards a business function, in this case the Organisation's marketing strategy.

19 The use of data directly in marketing is also a valid business purpose. But the intent and purpose are markedly different from statistical research. Marketing is intended to promote an organisation's products or services to new or existing customers. While I am no expert in marketing practices, what I do know is that the profiling of positive examples and the association of an organisation's products or services with success stories is not an uncommon practice. Its effectiveness is a question that each organisation that chooses to adopt such a practice needs to be satisfied with and is not within the domain of personal data protection laws. What is within the domain of personal data protection laws is whether the individual whose image and other personal data will be used has consented to such use, or whether there is some other lawful justification that an organisation may rely upon. In this regard, the various Facebook posts published by the Organisation clearly identified students individually and showed their details on an individual basis. It is clear that the Organisation's aim of profiling these individuals was for marketing purposes with the intent to promote its services to new (or even existing) customers. In the premises, I do not think that the purpose for which such personal data was disclosed can reasonably be said to fall within a "compilation" or "analysis of statistics" for marketing purposes. On the contrary, the personal data was used directly as part of the Organisation's marketing campaign by featuring success stories. Parenthetically, I had intimated in my earlier decision in *Re My Digital Lock Pte Ltd*[6] that this is an area where there is overlapping coverage between personal data protection law and the laws protecting privacy, specifically personality rights that may be protected under

6 [2017] PDP Digest 146.

defamation law. In the present case, I have confined my analysis to breaches of the Consent and Notification Obligations under the PDPA.

20 The student handbook also contained the following cl 15.5:

> 15.5 By attending school activities & event, you consent to the use of your photograph, voice, likeness, and image in any broadcasts of this event and in subsequent productions drawn from video or audio recordings of this event. The photographs and recordings may be published or broadcasted in the official SCI and affiliates' publications and in publicity materials, including the SCI and affiliates' websites and social media …

21 As cl 15.5 of the student handbook refers to "photographs" and "publicity materials", the Organisation could arguably rely on this clause of the student handbook for consent to post photographs of students on its Facebook page for publicity purposes, if such photographs were taken at events organised by the Organisation. The purposes that are notified by cl 15.5 relates to how the Organisation may use video footage and photographs of its activities for publicity purposes. For such purposes, the primary focus is on the activities of the Organisation and the involvement of the individual students is secondary (although it may not be incidental or minor). The intent is to create favourable impressions of the Organisation by featuring its activities and perhaps even its students' achievements in sporting and other activities. This purpose is markedly different from profiling selected students and associating their academic achievements with the Organisation. In this type of use, the student becomes the subject and the focus. Where the student becomes the subject and the purpose is to associate his or her academic achievement with the commercial objectives of the Organisation, specific consent ought to be obtained, and this ought to be obtained from his or her parent or guardian, as the purpose of use has probably crossed into commercial use. Moreover, this clause of the student handbook would not cover the disclosure of other personal data on the Organisation's Facebook page, such as students' names, date of birth, school assigned to and level of study.

22 In the light of the above, it follows that the Organisation has not complied with its Notification Obligation under s 20 of the PDPA to inform the parents or guardians of its students, who are minors, of the purpose(s) for which the Organisation disclosed its students' personal data on its Facebook page, in respect of Posts A, B, C and D minimally. The Organisation has, therefore, breached its Consent Obligation under

s 13 of the PDPA to obtain consent from such minors' parents or guardians for the same.

23 Further, given the finding that the Organisation has not complied with its Notification Obligation under s 20 of the PDPA, the Organisation is also in breach of s 18 of the PDPA.

The Organisation's follow-up remedial actions

24 As mentioned above, the Organisation took steps to remove Post A from its Facebook page and to make the post non-indexable by online search engines. Sometime after the aforementioned breaches had occurred, the Organisation represented that it had "created" a "Marketing Consent and Release Form" ("MRF"), which the Organisation then instructed its staff to use in order to obtain consent for using students' personal data for marketing purposes.

25 An extract from the MRF reads:

> I, _____ (name), _____ (NRIC) *irrevocably* authorize the school, its employees, and its agents, to use my / my child's name, information, picture, and likeness as recorded by the school for *any purpose* that the school deems appropriate, including promotional or advertising efforts. I specifically authorize the school, its employees, and its agents, to use, reproduce, exhibit, or distribute my / my child's name & information and likeness for such purpose in any communications medium currently existing or later created, including without limitation print media, television, and the Internet. [emphasis added]

26 The MRF purports to give the Organisation a very broad discretion to use students' information, by using the catch-all phrase "for any purpose that the school deems appropriate". In this respect, apart from the accompanying words "including promotional or advertising efforts", the MRF does not provide individuals with any greater specificity or details as to the purposes for which the Organisation may use their personal data.

27 It falls on me to highlight the following passage from the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, which would be pertinent in this instance:[7]

> [I]f an organisation's Data Protection Policy sets out its purposes in very general terms (and perhaps for a wide variety of services), it may need to provide a *more specific description of its purposes* to a particular individual who will be providing his personal data in a particular situation (such as when subscribing for a particular service), *to provide clarity to the individual on how his personal data would be collected, used or disclosed.* [emphasis added]

28 In my view, the language used in the MRF is so broad that it cannot reasonably be said to provide adequate clarity to individuals on the purposes for which their personal data would be used, and does not fulfil the requirements of s 20 of the PDPA.

29 Additionally, I note from the extract of the MRF as set out in [25] above, that the MRF purports to "irrevocably authorize" the Organisation to use students' personal data for "any purpose that the school deems appropriate". Needless to say, an overly-broad consent clause like this is unlikely to stand up to scrutiny and will probably not be effective in notifying purpose and thus any consent obtained in reliance on it rests on weak foundations. Furthermore, this provision in the MRF is potentially contrary to the requirements of s 16 of the PDPA:

(a) s 16(1) of the PDPA provides that individuals may at any time withdraw any consent given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose; and

(b) s 16(3) of the PDPA further provides that an organisation must not prohibit an individual from withdrawing such consent.[8]

30 In my view, the provision in the MRF that the Organisation be "irrevocably" authorised to use students' personal data effectively seeks to prohibit such individuals from withdrawing their consent to the use of their personal data. Supposing that the MRF had been obtained by the

---

7 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 14.13.

8 Section 16(3) of the Personal Data Protection Act 2012 (Act 26 of 2012) further provides that this section does not affect the legal consequences arising from such withdrawal.

Organisation from the students' parents or guardians in this case, I may not have hesitated to find that it is ineffective as being contrary to the requirements under s 16 of the PDPA. However, I am also mindful of other circumstances where an irrevocable promise may be permissible, for example, in a professional modelling agreement an individual executes an irrevocable release in return for modelling fees from an advertisement agency for a specific client's marketing campaign, in which case the bargain that is struck ought to be respected. The analysis would involve a detailed discussion of the interaction of the consent provisions of the PDPA and contractual principles. But this is not an analysis for this case nor do I need to reach such a conclusion in these grounds.

31 In the final analysis, I do not think that the MRF validly notifies the parents or guardians of the minors of the specific marketing use of their child or ward's personal data, nor is it acceptable in its current form for use in the context of the present pedagogical relationship between the Organisation and its students, as it purports to provide for an irrevocable waiver of the students' right to withdraw their consent, which is contrary to s 16 of the PDPA.

DIRECTIONS

32 Having found that the Organisation is in breach of ss 13 and 18 of the PDPA, I am empowered under s 29 of the PDPA to give the Organisation such directions as I deem fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1m.

33 In assessing the breach and determining the directions to be imposed on the Organisation, I took into account the following factors in its mitigation:

(a) there was no complaint or allegation received to the effect that there was any loss or damage accruing to individuals as a result of the Organisation's breach;

(b) the Organisation demonstrated a willingness to take remedial actions upon being informed of the breach by the Complainant; and

(c) the Organisation was generally co-operative throughout the investigation process and did not seek to obfuscate its role or the facts in this matter.

34 In consideration of the relevant facts and circumstances of the present case, I hereby direct the Organisation to:

(a) remove Posts B, C and D, and any other posts of a similar nature for which consent had not been obtained from the relevant individuals for their personal data to be used and disclosed on the Organisation's Facebook page;

(b) revise the MRF and all other documents used by the Organisation for obtaining consent from its students for the collection, use and disclosure of its students' personal data, taking care:

(i) to provide sufficient clarity and avoid the use of "catch-all" phrases in the articulation of the purposes for which personal data would be collected, used and disclosed;

(ii) in particular, where the Organisation collects, uses or discloses personal data for purposes that involve marketing and profiling, to ensure that consent be obtained specifically for those purposes; and

(iii) to clarify that individuals are not prohibited from withdrawing their consent; and

(c) take all other steps and make such other arrangements as would reasonably be required to meet (a) and (b) above.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Flight Raja Travels Singapore Pte Ltd

[2019] PDP Digest 243

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1705-B0730
Decision Citation: [2019] PDP Digest 243; [2018] SGPDPC 16

Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

11 June 2018

1 This complaint concerns a user of Flight Raja Travels Singapore Pte Ltd's (the "Organisation") online travel booking system (the "Booking System"). While using the Booking System, the user was able to access information of other users (the "Incident").

2 What happened was that after the user resumed his session after time-out, the Booking System showed him 45 sets of booking records. The booking records accessed by the user contained the personal data of 72 other individuals. This included name, passport number, booking ID, flight details (including the flight number, departure/arrival date, time and airport), booking date, amount paid, and flight inclusions.

3 Investigations were commenced under s 50 of the Personal Data Protection Act 2012[1] (the "PDPA"). The material facts of the case are as follows.

4 Up to December 2016, the Booking System was accessed through browser login via the Organisation's website. The Organisation then introduced a new application (the "New Mobile App"). The New Mobile App enabled access through mobile devices without login. It recognised the mobile device IDs of registered users stored as part of their account information.

1 Act 26 of 2012.

5 Proper change management would have included full system integration testing of the New Mobile App with the Booking System to detect any unintended effects from the changes. However, two unintended effects went undetected. They affected non-registered users who had just completed a booking via the Booking System through a browser and had been registered by the Booking System as new users ("Newly Registered Users").

6 The first unintended effect was to change the behaviour of the Booking System when Newly Registered Users resumed their sessions following a time-out. A time-out occurred if their sessions happened to be idle for 30 minutes. The System no longer redirected them to the homepage as it did before the changes. Instead, they stayed on the same page where they could access the "Dashboard".

7 The second unintended effect was when the timed-out Newly Registered Users accessed the Dashboard tabs. The Dashboard's "past", "upcoming" and "all" tabs disclosed the records of bookings by other individuals. Each tab could display a maximum 15 records, thereby disclosing a total of 45 records.

FINDINGS AND BASIS FOR DETERMINATION

8 The complaint pertains to the protection obligation under s 24[2] of the PDPA. In the context of the present case, when an organisation makes changes to a system that processes personal data in its possession or control, the organisation has to make reasonable arrangements to prevent any compromise to personal data.

9 The Organisation omitted to test the effects of access through the New Mobile App with the existing access through browsers. Registered Users are identified by their mobile device IDs that are associated with their user account. However, Newly Registered Users who completed bookings through browsers had no mobile device IDs stored in their accounts.

---

2 Section 24 of the Personal Data Protection Act 2012 (Act 26 of 2012) requires an organisation to protection 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 risk.

10 An integration test plan should have considered whether such Newly Registered Users could be identified by other information in their accounts. However, in the absence of mobile device ID in a Newly Registered User's account, the browser retrieved and displayed other booking records in the Dashboard tabs as mentioned above.

11 Further, session time-out was a likely occurrence. This included time-out of browser sessions of Newly Registered Users. An integration test plan ought to have anticipated this scenario. The Organisation was therefore found in breach of s 24 of the PDPA.

12 Having found that the Organisation is in breach of the PDPA, I am empowered under s 29 of the PDPA to issue the Organisation such directions as it deems fit to ensure compliance with the PDPA. In assessing the impact of the breach, I considered the fact that a specific set of circumstances was needed for the disclosure to have occurred, and such a coincidence is uncommon:

(a) the user had never registered on the Website previously;
(b) the user made a booking and made payment;
(c) the user did not log out or close the browser window but instead left the page idle for 30 minutes;
(d) the user returned to the same webpage after 30 minutes; and
(e) the user clicked on the dashboard hyperlink.

13 The disclosure occurred only if payment had been made for one or more travel tickets. This meant that disclosure would likely have been to *bona fide* customers rather than other persons. Additionally, the nature of the flaw made it less readily detectable by an attacker, compared with misconfigured firewalls or unpatched servers, for instance.

14 Further, I considered that disclosure to the complainant was limited to 45 sets of booking records disclosed. At a maximum, the bug exposed a total of 72 personal data sets of booking information.

15 Accordingly, I hereby direct the Organisation to carry out the following within 60 days:

(a) assess whether its application testing has been complete in order to discover and remedy any risk to personal data from the changes made to introduce the new mobile application function;
(b) furnish a report of the assessment as well as action taken in response; and

(c) to put in place procedures and processes to manage the risks to the personal data in its possession or control, when making changes to its applications, by implementing testing procedures and documenting the tests conducted.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Singapore Taekwondo Federation

[2019] PDP Digest 247

Coram: Tan Kiat How, Commissioner
Case Number: DP-1705-B0810
Decision Citation: [2019] PDP Digest 247; [2018] SGPDPC 17

Openness Obligation *– Failure to designate one or more persons to be responsible for ensuring that Organisation complies with Personal Data Protection Act 2012 (Act 26 of 2012)*
Openness Obligation *– Lack of data protection policies and practices*
Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

22 June 2018

BACKGROUND

1 This matter involves the Singapore Taekwondo Federation (the "Organisation"), a society registered with the Registry of Societies that is responsible for promoting, supporting, and developing taekwondo-related programmes and activities in Singapore.

2 Since 2015, the Organisation has been posting, on an annual basis, PDF documents which contain the names and schools of students who are participants of the Annual Inter-School Taekwondo Championships ("Championships") on the Organisation's website which is accessible to the general public. It was represented by the Organisation that the purpose of uploading the PDF documents on its website was to enable students to verify their participation in the Championships.

3 On 30 May 2017, a complaint was lodged by a member of the public ("Complainant") with the Personal Data Protection Commission ("Commission"), alleging that there was an unauthorised disclosure of the NRIC numbers of 782 students who were participants of the 2017 Championships. Whilst the NRIC numbers, within the PDF documents,

were set out in columns that were minimised and not immediately visible, there was an unauthorised disclosure of these NRIC numbers when the Complainant subsequently copied and pasted the contents of the PDF documents onto another document.

4 The Commissioner sets out below his findings and grounds of decision based on the investigations carried out in this matter.

MATERIAL FACTS

5 On 19 May 2017, the Complainant chanced upon the PDF documents on the Organisation's website, which contained the names and schools of students who were participants of the 2017 Championships.

6 The NRIC numbers of the students were not immediately visible to the Complainant in the PDF documents, as the NRIC numbers were set out in columns which were minimised. Nevertheless, when the Complainant copied and subsequently pasted the contents of the PDF documents onto another document, he was able to view the NRIC numbers of the students. The Complainant proceeded to inform the Organisation of this unauthorised disclosure of the students' NRIC numbers via e-mail on 19 May 2017.

7 As the Complainant did not receive any response from the Organisation, he proceeded to lodge a complaint with the Commission on 30 May 2017. Upon receiving the complaint, the Commission commenced an investigation into this matter.

8 On 31 May 2017, after the Organisation was notified by the Commission of the unauthorised disclosure of the students' NRIC numbers, the Organisation removed the PDF documents from its website. The Organisation represented that it had also taken steps to contact Google to remove the cache, as well as instructed its staff to delete the relevant information in question before uploading any documents on to the Organisation's website.

9 During the course of the Commission's investigation, the Organisation made the following representations in relation to its process of handling the personal data of the students intending to participate in the Championships. Firstly, it would receive an encrypted Excel spreadsheet containing the personal data of students intending to participate in the

Championships, including their names, NRIC numbers, dates of birth, gender, school, class, taekwondo grade, names of taekwondo instructors and clubs, from the Physical Education Sport Education Board of the Ministry of Education ("MOE").

10 After receiving the encrypted Excel spreadsheet, the Organisation's Head of the Tournament Department ("Tournament Head") would typically proceed to rearrange the students' personal data into programme lists and bout sheets using Microsoft Excel. The Tournament Head asserted that in relation to the Excel spreadsheets containing the students' personal data, he would "hide" their NRIC numbers, before converting the Excel spreadsheets into PDF documents.

11 The Tournament Head describes the process as follows:

> I will copy and paste the names, NRIC numbers, and schools into a new excel spreadsheet. I will then *hide* the NRIC numbers and then add in the programmes into the new excel spreadsheet. I have been doing this since 2015.
>
> Thereafter, I will send the new excel spreadsheet with the names, schools, programme list and hidden NRIC numbers to [redacted] who will then convert it into a PDF list for uploading onto STF's website. She also has been doing this since 2015 but she does not know that I simply hide the NRIC numbers.
>
> [emphasis added]

12 The investigation carried out by the Commission sought to verify the assertion made by the Tournament Head. A check on the Internet, including the website of Adobe Systems Incorporated, the proprietor of the Adobe PDF software, did not reveal the reappearance of "hidden" contents when copied to a separate Microsoft Word or Excel document ("Alleged Bug") to be a known issue or function.

13 In addition, officers of the Commission had conducted tests to replicate the result of the Alleged Bug. The officers of the Commission first copied the PDF documents in question found on the Organisation's website to a newly created Microsoft Word document and found that the columns which were not visible on the PDF documents appeared when copied to the Microsoft Word document. This verified the Complainant's assertion. However, when the officers of the Commission created a new Excel spreadsheet with properly hidden columns, this Alleged Bug did not occur. Subsequently, the officers of the Commission discovered that this

issue would only occur if the columns were minimised instead. In other words, if the columns in an Excel spreadsheet were minimised instead of hidden, and the Excel spreadsheet were to be converted into PDF format, then the contents of the minimised columns would reappear when the PDF document was copied onto a Microsoft Word or Excel document.

14 Based on the foregoing, the Commissioner finds that the columns in the Excel spreadsheet prepared by the Tournament Head were not hidden but merely minimised.

15 In relation to the reason for purportedly hiding (but actually minimising) the column with NRIC numbers in the Excel spreadsheet, the Organisation represented that this was for the sake of convenience in submitting the results of the Championships to participating schools. Following the conclusion of the Championships, participating schools would typically request for the name lists of the medallists and the results of the Championships, which would have to contain the students' NRIC numbers, so as to allow the schools to verify and present colour awards to their students.

16 The Organisation conceded that it was not aware that there were columns which had been minimised in the PDF documents, such that the NRIC numbers in these columns appeared when the contents of the PDF documents were copied and pasted to another document.

17 In addition, the Organisation admitted during the course of the investigation that it was not aware of the Personal Data Protection Act 2012[1] ("PDPA"). Consequently, the Organisation did not appoint a data protection officer ("DPO"), nor did it implement any policies or practices necessary for it to meet its obligations under the PDPA.

FINDINGS AND BASIS FOR DETERMINATION

18 The issues for determination are as follows:

(a) whether the Organisation had complied with its obligation under s 11 of the PDPA to designate one or more persons to be responsible for ensuring that the Organisation complies with the PDPA;

1 Act 26 of 2012.

(b) whether the Organisation had complied with its obligation under s 12 of the PDPA to develop and implement policies and practices that are necessary for the Organisation to meet its obligations under the PDPA; and

(c) whether the Organisation had complied with its obligation under s 24 of the PDPA to implement reasonable security arrangements to protect personal data in the Organisation's possession or under the Organisation's control.

19 At the outset, although the Tournament Head represented during the investigation that the Organisation is managed mostly by a team of volunteers, pursuant to s 53(1) of the PDPA, the Organisation would be responsible for its employees' (which includes volunteers[2]) actions which are engaged in the course of their employment.[3]

20 In addition, the NRIC numbers that were disclosed constitutes personal data as defined in s 2(1) of the PDPA, as every single student in the PDF documents could be identified from the NRIC numbers disclosed. Accordingly, the Organisation would be subject to the data protection obligations under Pts III to VI of the PDPA.

Nature of personal data

21 As a preliminary issue, the Commissioner first considered the nature of the personal data in this matter.

22 The personal data disclosed NRIC numbers which, according to the Commission's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[4] ("Key Concepts Guidelines") and the *Guide to Basic Data Anonymisation Techniques*[5] ("Anonymisation Guide"), constitute a data attribute that is assigned to an individual for the purposes of identifying the

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

3 Section 53 read with s 4(1)(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012).

4 Revised on 27 July 2017.

5 Published on 25 January 2018.

individual and, on its own, identifies an individual.[6] The Commission's *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*[7] ("Selected Topics Guidelines") also recognise that "NRIC numbers are of *special concern* to individuals as they are *unique* to each individual" [emphasis added].[8]

23 In addition, the NRIC numbers that were disclosed were the NRIC numbers of students, minors who were less than 21 years of age. The Selected Topics Guidelines recognise that certain considerations may arise in this regard, including that "there is generally *greater sensitivity* surrounding the treatment of minors" [emphasis added].[9] Therefore, good practices in protecting minors' personal data include, amongst other things, placing "*additional* safeguards against [the] unauthorised disclosure of, or unauthorised access to, [the] personal data of minors" [emphasis added].[10]

24 A similar approach in respect of minors' personal data has been adopted in several other jurisdictions. In Canada, the Office of the Privacy Commissioner of Canada ("OPC") has expressed that it "has consistently viewed personal information relating to youth and children as being *particularly sensitive* and must be handled accordingly" [emphasis added].[11]

25 In the UK, the Information Commissioner's Office ("ICO") has taken the view that "children need *particular protection* when [an organisation is] collecting and processing their personal data" [emphasis added] and if an organisation processes children's personal data, the organisation "should think about the need to protect them from the outset,

---

6 Personal Data Protection Commission, *Guide to Basic Data Anonymisation Techniques* (25 January 2018) at para 3.1 and Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 5.9.

7 Revised on 28 March 2017.

8 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at para 6.1.

9 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at para 8.12.

10 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at para 8.12.

11 Office of the Privacy Commissioner of Canada, "Guidance for businesses that collect kids' information" (3 November 2017).

and design [the organisation's] systems and processes with this in mind".[12] The ICO has also expressed that there are "*important additional considerations* that need to [be taken] into account when [an organisation's] data subject is a child" [emphasis added].[13]

26 In Hong Kong, the Office of the Privacy Commissioner for Personal Data ("PCPD") has taken the view that "children are identified as a *vulnerable* group who may have *special needs* in privacy protection" [emphasis added].[14]

27 Against this backdrop, it is evident that minors' personal data would typically be of a more sensitive nature, especially when it concerns unique identifiers such as NRIC numbers. Accordingly, when it comes to the protection of "sensitive" personal data, organisations are required to take extra precautions and ensure higher standards of protection under the PDPA.

Whether the Organisation had complied with its obligations under section 11 of the Personal Data Protection Act

28 At the outset, during the investigation, the Organisation admitted that it had "no idea of the PDPA", and consequently, was not aware of its data protection obligations under Pts III to VI of the PDPA.

29 Notably, the Organisation's lack of awareness of its data protection obligations is not a legitimate defence to a breach under the PDPA, as set out in *Re M Stars Movers & Logistics Specialist Pte Ltd*[15] ("*M Stars Movers*") at [16]:

> It is a trite principle of law that ignorance of the law is no excuse. Thus, the Organisation's lack of awareness of its obligations under the PDPA cannot

12 UK Information Commissioner's Office, "Children" <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/> (accessed 23 April 2019).

13 UK Information Commissioner's Office, "What Do We Need to Consider When Choosing a Basis for Processing Children's Data?".

14 Hong Kong, Office of the Privacy Commissioner for Personal Data, "2015 Study Report on Online Collection of Children's Personal Data" (December 2015).

15 [2018] PDP Digest 259.

> excuse its breach of the PDPA. The data protection provisions of the PDPA took effect on 2 July 2014 after a 'sunrise' period of more than a year from 2 January 2013. Since then, organisations have had ample opportunities to develop and implement appropriate policies and practices to comply with the PDPA. In any event, an organisation's lack of awareness of its data protection obligations is not a legitimate defence to a breach.

30 Section 11(3) of the PDPA requires the Organisation to designate one or more individuals, *ie*, the DPO, to be responsible for ensuring the Organisation's compliance with the PDPA.

31 The Organisation confirmed that there was "no person appointed for the role of Data Protection Officer".

32 By the Organisation's own admission, the Commissioner finds that the Organisation has failed to meet its obligations under s 11(3) of the PDPA. The Commissioner repeats the comments at para 29 above that a lack of awareness of the obligations imposed by the PDPA does not amount to a legitimate defence against a breach by the Organisation.

33 The Commissioner takes this opportunity to reiterate the importance of the role of a DPO as set out in *M Stars Movers*:[16]

> The DPO plays an important role in ensuring that the organisation fulfils its obligations under the PDPA. Recognition of the importance of data protection and the central role performed by a DPO has to come from the very top of an organisation and ought to be part of enterprise risk management frameworks … The DPO ought to be appointed from the ranks of senior management and be amply empowered to perform the tasks that are assigned to him/her … The DPO need not – and ought not – be the sole person responsible for data protection within the organisation … Every member of staff has a part to play …

34 Generally, the responsibilities of a DPO include, but are not limited to:[17]

(a) ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data;

---

16 *Re M Stars Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 at [33].

17 Personal Data Protection Commission, "Data Protection Officers" <https://www.pdpc.gov.sg/Organisations/Data-Protection-Officers> (accessed 20 April 2019).

(b) fostering a data protection culture in an organisation and communicating personal data protection policies to stakeholders;
(c) handling and managing personal data protection related queries and complaints;
(d) alerting management to any risks that may arise with regard to personal data; and
(e) liaising with the Commission on data protection matters, if necessary.

35 From the foregoing, it is clear that the DPO plays a vital role in implementing and building a robust data protection framework to ensure an organisation's compliance with its obligations under the PDPA.

Whether the Organisation had complied with its obligations under section 12 of the Personal Data Protection Act

36 Section 12(*a*) of the PDPA requires an organisation to develop and implement policies and practices that are necessary to meet its obligations under the PDPA.

37 During the investigation, the Organisation confirmed that there was "no personal data policy" implemented and represented that the manner of handling the students' personal data was an "unwritten SOP".

38 By the Organisation's own admission, the Commissioner finds that the Organisation has failed to meet its obligations under s 12(*a*) of the PDPA. Similar to the above, the Commissioner repeats his comments at [29] that a lack of awareness of the obligations imposed by the PDPA does not amount to a legitimate defence against a breach by the Organisation.

39 The Commissioner takes this opportunity to reiterate the role of data protection policies, as set out in *Re Aviva Ltd*[18] at [32]:

> … Data protection policies and practices developed and implemented by an organisation in accordance with its obligations under section 12 of the PDPA are generally meant to increase awareness and ensure accountability of the organisation's obligations under the PDPA …

18 [2018] PDP Digest 245.

40 In addition, *M Stars Movers* highlights the importance of the need for organisations to develop and implement data protection policies and practices:[19]

> 27 At the very basic level, an appropriate data protection policy should be drafted to ensure that it gives a clear understanding within the organisation of its obligations under the PDPA and sets general standards on the handling of personal data which staff are expected to adhere to. To meet these aims, the framers, in developing such policies, have to address their minds to the types of data the organisation handles which may constitute personal data; the manner in, and the purposes for, which it collects, uses and discloses personal data; the parties to, and the circumstances in, which it discloses personal data; and the data protection standards the organisation needs to adopt to meet its obligations under the PDPA.
>
> 28 An overarching data protection policy will ensure a consistent minimum data protection standard across an organisation's business practices, procedures and activities …

41 Finally, the Commissioner reiterates past observations on the benefits and importance of documenting an organisation's data protection policies and practices in a written policy, as per *Re Furnituremart.sg*:[20]

> The lack of a written policy is a big drawback to the protection of personal data. Without having a policy in writing, employees and staff would not have a reference for the Organisation's policies and practices which they are to follow in order to protect personal data. Such policies and practices would be ineffective if passed on by word of mouth, and indeed, the Organisation may run the risk of the policies and practices being passed on incorrectly. Having a written policy is conducive to the conduct of internal training, which is a necessary component of an internal data protection programme.

42 It is clear from the foregoing that the development and implementation of written data protection policies and procedures are important in ensuring an organisation's compliance with its obligations under the PDPA.

---

19 *Re M Stars Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 at [27]–[28].

20 [2018] PDP Digest 175 at [14].

Whether the Organisation had complied with its obligations under section 24 of the Personal Data Protection Act

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

44 The Commissioner's assessment of whether the Organisation had complied with its obligations under s 24 of the PDPA would be confined to the NRIC numbers of students. As admitted by the Organisation during the course of the investigation, the NRIC numbers of students were not supposed to be contained and disclosed in the PDF documents.

45 Whilst the encrypted Excel spreadsheet containing the students' personal data was provided by the MOE, the entire process of compiling the personal data into a separate Excel spreadsheet, converting the Excel spreadsheet into PDF documents and uploading the PDF documents were actions that were conducted solely by the Organisation, without any external interference from the MOE or the entity responsible for maintaining the Organisation's website.

46 That said, the Organisation was unaware and unable to explain why the NRIC numbers were left in the minimised columns in the PDF documents.

47 In this regard, the Organisation's mistake of not realising that the NRIC numbers were present in minimised columns in the PDF documents and could have been disclosed without authorisation could be quite easily repeated. Any person could simply copy the contents of the PDF documents and paste them onto another document, thereby resulting in further unauthorised disclosures of the students' personal data. Such potential impact and harm cannot be ignored, especially when it involves the NRIC numbers of 782 students who were also minors, and whose personal data would thus be considered to be more sensitive in nature.

48 It is precisely the fact that the unauthorised disclosure could have reoccurred quite easily due to the same mistake, that focus is drawn to the issue of whether the Organisation had complied with its obligations under s 24 of the PDPA.

49 On this issue, the Commission found that the Organisation did not appear to have taken sufficient steps towards protecting the personal data in its possession, to prevent the unauthorised disclosure of the personal data.

50 An example of an administrative security arrangement which the Organisation could have made in respect of the personal data in its possession, was to "[c]onduct regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data".[21] The Organisation could have implemented staff training sessions to "[e]nsure that staff are trained and familiar with the software used to process … documents containing personal data. For example, staff using spreadsheets should be aware of how sorting the data incorrectly may lead to errors".[22] Similarly, the Organisation could have adopted any of the following measures to ensure that personnel using Microsoft Excel to process personal data were well apprised of and updated on the functions of the software, in particular, the difference between columns that were "minimised" and "hidden" in an Excel spreadsheet:

(a) "[e]nsure that new and existing staff receive regular training so that they are well apprised and updated on the proper procedures for processing and sending personal data";[23]

(b) "[train] staff to ensure only necessary personal data are extracted";[24]

(c) "[k]eep ICT security awareness training for employees updated and conduct such training regularly";[25] and

---

21 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 17.5.

22 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* (20 January 2017) at para 2.1.

23 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* (20 January 2017) at para 2.2.

24 Personal Data Protection Commission, *Guide to Data Protection Impact Assessment* (1 November 2017) at para 7.2.

25 Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017) at para 5.2.

(d) "[provide] the appropriate training to ensure proper usage of the software used".[26]

51 Given the nature of the personal data in question, the Organisation had not taken into consideration what extra precautions would be required to protect the sensitive personal data of the students, who are minors.

52 The Key Concepts Guidelines express that an organisation should "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity".[27] As set out in the Commission's *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data*, "[d]ocuments or communications that contain sensitive personal data should be processed … with *particular care*" [emphasis added].[28]

53 The Selected Topics Guidelines goes on to state that (at [8.12]):

> … given that there is generally greater sensitivity surrounding the treatment of minors, it may be prudent for organisations to consider putting in place relevant precautions, if they are (or expect to be) collecting, using or disclosing personal data about minors. For example, organisations that provide services targeted at minors could state terms and conditions in language that is readily understandable by minors, or use pictures and other visual aids to make such terms and conditions easier to understand. Other good practices could include placing additional safeguards against unauthorized disclosure of, or unauthorized access to, personal data of minors, or anonymising personal data of minors before disclosure, where feasible.

54 In this regard, the Commissioner agrees with the OPC that, in the context of children's personal data, safeguards that are implemented must be "commensurate with the amount and potential sensitivity of the information at risk" and if the appropriate safeguards are not implemented, this "could, in the wrong hands, put children at unnecessary risk of

---

26 Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017) at para 17.7.

27 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 17.3.

28 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* (20 January 2017) at para 2.2.

harm".[29] In that case, the OPC found that the personal data of approximately 316,000 Canadian children, in addition to approximately 237,000 Canadian adults, that were in the possession of a toy manufacturer had been compromised as the organisational and technological safeguards that were implemented at the time of the data breach incident were not commensurate with the amount and potential sensitivity of the personal data.

55 When it comes to the protection of "sensitive" personal data, the Organisation had failed to take extra precautions to guard against and prevent unauthorised disclosures of personal data, and failed to ensure a relatively higher standard of protection of personal data under the PDPA. At a minimum, the Organisation ought to have ensured that its staff in charge of creating, processing and converting the Excel spreadsheets were given proper and regular training to equip them with the knowledge to utilise the correct function to convert the Excel spreadsheets into PDF documents that were routinely published on the Organisation's website.

56 Not only did the Organisation fail to develop and implement the appropriate security arrangements upon the PDPA coming into full force on 2 July 2014, this failure had carried on well after 2 July 2014. Considering how there were two other instances where the Organisation had uploaded the personal data of students in the same manner, specifically for the 2015 and 2016 Championships, the Organisation's prolonged failure to develop and implement reasonable security measures (for instance, in the form of proper and regular staff training to equip staff with the knowledge to use the right Microsoft Excel feature) to protect the personal data is also taken into consideration in this decision.

57 Given the absence of any security arrangements to protect personal data in its possession against unauthorised disclosure, the Commissioner finds that the Organisation has contravened s 24 of the PDPA.

---

29 Office of the Privacy Commissioner of Canada, "PIPEDA Report of Findings #2018-001: Connected Toy Manufacturer Improves Safeguards to Adequately Protect Children's Information" (8 January 2018) at "Overview".

DIRECTIONS

58 Having found that the Organisation is in breach of ss 11, 12 and 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

59 In assessing the breach and determining the directions to be imposed on the Organisation, the Commissioner took into account, as a mitigating factor, the Organisation's prompt remedial actions to rectify and prevent the recurrence of the data breach.

60 The Commissioner also took into account the following aggravating factors:

(a) the personal data disclosed involved the NRIC numbers of minors, which constitute personal data of a sensitive nature, and the disclosure of which could cause substantial actual or potential harm to the students;
(b) the Organisation showed a lack of awareness of its obligations under the PDPA; and
(c) the Organisation caused quite some delays in the investigation process. Despite the approval of an extension of time for responding to the Commission's Notice to Require Production of Documents and Information issued under the Ninth Schedule of the PDPA, the Organisation only responded after the Commission had sent subsequent reminders requesting for the Organisation's response, and only after the president of the Organisation was copied in one of such e-mail reminders.

61 The Commissioner has also reviewed the representations made by the Organisation seeking a reduction in the financial penalty imposed, a summary of which follows:

(a) the Organisation is a small registered charity with a thin budget;
(b) the Organisation did not appoint a data protection officer and as such was unaware of the requirement to have a data protection policy;
(c) the Organisation took immediate remedial action;
(d) the breach was due to inadvertence and ignorance that the NRIC data could be seen on its website;

(e) the Organisation acknowledged the unauthorised disclosure of 782 students but that there is no specific information to suggest that the data of the students involved in the 2015 and 2016 tournaments had been similarly disclosed; and

(f) the delay was caused by its surprise at the lapse and its need to obtain external advice as well as the Organisation's internal approval process to respond to the PDPC.

62 It should be noted that the Commissioner had already taken (c) above into consideration in determining the financial penalty quantum. The Commissioner finds that the rest of the above representations do not justify a reduction in the financial penalty. The PDPA applies to all organisations and the mere fact that the Organisation is a small charity is not a mitigating factor. If the Organisation has cash flow issues, it is open to the Organisation to request that the penalty be paid in instalments. Also, inadvertence and ignorance of the law are not mitigating factors.

63 On the point of delay, the Organisation took two months to respond to the first Notice to Produce issued to the Organisation. The initial deadline to respond to the Notice to Produce was on 23 June 2017, two weeks after the Notice to Produce was issued. PDPC granted the Organisation's request for an extension of time to respond to the Notice to Produce by 31 July 2017. The Organisation failed to meet this extended deadline and did not respond even after a first reminder was sent on 2 August 2017. The Organisation only responded to the Notice to Produce after a second reminder was issued on 10 August 2017 and copied to the president of the Organisation. The Organisation had already been granted the requested five-month extension of time to respond and failed to do so within that time, only responding after two reminders were issued. The Commissioner finds that the seven weeks given to the Organisation to respond was more than sufficient to engage third-party experts to assist the Organisation in its investigations and to obtain the necessary internal approval. The delay was therefore unacceptable.

64 In consideration of the relevant facts and circumstances of the present case, the Commissioner hereby directs the Organisation to:

(a) pay a financial penalty of S$30,000 within 30 days from the date of this direction, failing which interest, at the rate specified

in the Rules of Court[30] in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty;

(b) appoint a DPO within 30 days from the date of this direction;

(c) develop and implement policies and practices that are necessary for the Organisation to meet its obligations under the PDPA within 30 days from the date of this direction; and

(d) inform the Commission of the completion of each of the above directions in (b) and (c) within one week of implementation.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

30 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Management Corporation Strata Title Plan No 4436

[2019] PDP Digest 264

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1711-B1315 and DP-1711-B1316
Decision Citation: [2019] PDP Digest 264; [2018] SGPDPC 18

Access and Correction Obligations *– CCTV footage – Subordination clause in PDPA – No requirement to redact personal data of other individuals under section 47 Building Maintenance and Strata Management Act (Cap 30C, 2008 Rev Ed)*

2 August 2018

BACKGROUND

1 The complaint concerns the Management Corporation Strata Title Plan No 4436 (the "Organisation") of River Isles Condominium ("River Isles") permitting a subsidiary proprietor to view the CCTV footage in the security guardhouse in the presence of two council members but without the presence of a security supervisor. The Organisation is formed to manage the River Isles.

2 On 6 and 7 November 2017, two subsidiary proprietors of River Isles (collectively known as the "Complainants") complained that the Organisation had allowed a fellow subsidiary proprietor to view the CCTV footage without supervision, notwithstanding the presence of the two council members. The purpose for viewing was to locate a missing cat on 2 November 2017. The Complainants were concerned other individuals might be captured in the said CCTV footage.

3 The Complainants alleged there was no security supervisor nor staff of Savills Property Management Pte Ltd, the managing agent ("MA"), present during the viewing. Although two council members were in attendance, the Complainants were of the view that only security guards, the MA's staff or police could view the CCTV footage.

4 In its responses, the Organisation averred that s 47 of the Building Maintenance and Strata Management Act[1] ("BMSMA") applies. Section 47 states that any subsidiary proprietor has the right to ask for inspection as well as request for a copy of any other record or document in the possession of the Organisation. Consequently, the request to view the CCTV footage by the subsidiary proprietor was, according to the Organisation, an inspection of a document that was permitted under s 47 of the BMSMA.

5 In this case, it is not disputed that the individual who applied for and viewed the CCTV footage was a subsidiary proprietor at the material time. Investigations disclosed that the inspection of the CCTV footage was carried out on 2 November 2017 at about 2110hrs by the subsidiary proprietor in the presence of two council members. The CCTV footage that was inspected consisted footage of the lift lobby on 29 October 2017 and the subsidiary proprietor viewed it for about 20–30 minutes.

FINDING AND BASIS FOR DETERMINATION

6 This case concerns the operation of the subordination provision in s 4(6)[2] with respect to the access obligation under s 21[3] of the Personal Data Protection Act 2012[4] ("PDPA") and its interaction with a subsidiary proprietor's right to inspect and take copies of documents under s 47 of the BMSMA. In particular, the issues are:

(a) whether CCTV footage is considered a document or record under s 47 of the BMSMA; and

---

1 Cap 30C, 2008 Rev Ed.

2 Under s 4(6)(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012), unless otherwise expressly provided, the provisions of other written law shall prevail to the extent that any provision of Pts III to VI is inconsistent with the provisions of that other written law.

3 Section 21 of the Personal Data Protection Act 2012 (Act 26 of 2012) requires the organisation to provide access to personal data about an individual that is in its possession or under its control subject to exceptions enumerated in the Fifth Schedule or s 21(3). Pertinent to this case is s 21(3)(*c*), which limits the data subject's right of access where it is reasonably expected to reveal personal data about another individual.

4 Act 26 of 2012.

(b) whether the subordination provision in s 4(6)(*b*) of the PDPA applies to displace s 21 of the PDPA in respect of a subsidiary proprietor's request for documents and records under s 47 of the BMSMA.

Whether CCTV footage is a document under section 47 of the Building Maintenance and Strata Management Act

7 In the case of *Tan Hee Chye v MCST Plan No 395*[5] ("*Tan Hee Chye*"), relying on the definition of online Oxford Dictionaries, the Strata Titles Board ("STB") accepted that the "audio recordings" fell within the definitions of "document" and "record". STB viewed that MCST should make available the audio recordings for inspection under s 47 of the BMSMA.

8 It is trite law that the meaning of the word "document", given the broadest definition, is capable of accommodating any form or medium on which information can be recorded in a material form. The courts have held that documents include electronic documents like e-mails, audio and video files, and even storage media and recording devices like hard disks.[6] The Supreme Court's Practice Directions on electronic discovery enumerate a list of reasonably usable file formats for the production of electronic documents during discovery which includes file formats for both audio and video files.[7]

9 The present case deals with video files in the form of CCTV footage. Since audio recordings can come within the meaning of "document" or "record", I do not see any reason why a video record should be treated with any exception. Accordingly, I am of the view that CCTV footage should also fall within the ambit of documents or records to which a subsidiary proprietor has a right to inspect and take copies under s 47 of the BMSMA.

---

5 [2016] SGSTB 1.

6 See *Sanae Achar v Sci-Gen Ltd* [2011] 3 SLR 967 at [10].

7 See Pt V of the Supreme Court Practice Directions and Appendix E Pt 4.

The interaction of the access obligation under section 21 of the Personal Data Protection Act and a subsidiary proprietor's right to inspection under section 47 of the Building Maintenance and Strata Management Act

10 Section 47 of the BMSMA states that the Organisation shall make available for inspection any document or record in the custody or under the control of the Organisation.[8] As such, the Organisation has a legal obligation to provide inspection and copies of documents or records to any subsidiary proprietor under s 47 of the BMSMA.

11 Section 21 of the PDPA gives a data subject the right to access personal data about him that the Organisation has in its possession or under its control. The data subject's right of access is curtailed by ss 21(2) and 21(3). Section 21(2) absolves the Organisation from providing — "is not required to provide" (but presumably has a discretion to provide if it is reasonable to do so) — access in any of the situations enumerated in the Fifth Schedule. In contrast, s 21(3) is a mandatory injunction that prohibits the Organisation from providing access — "shall not provide" — in any of the situations enumerated therein. In the present case, the pertinent provision is s 21(3)(*c*). The Organisation cannot provide (and has no discretion in the matter) access to personal data that can reasonably be expected to reveal personal data about another individual. The Personal Data Protection Commission has issued advisory guidelines[9] on the operation of s 21 of the PDPA which requires organisations to redact personal data about other individuals from documents that are provided to a data subject pursuant to a data subject access request, unless consent for disclosure has been obtained from these other individuals.

12 The subordination provision in s 4(6)(*c*) of the PDPA becomes operative when there are inconsistencies between the provisions of any other written law and the provisions in Pts III to VI of the PDPA. It operates by placing the PDPA provisions in subordination to other written law, such that the provisions of such other written laws shall prevail in the event of any inconsistencies. In the present case, the two potentially inconsistent provisions are s 47 of the BMSMA and s 21 of the PDPA.

---

8 See *Tan Hee Chye v MCST Plan No 395* [2016] SGSTB 1.

9 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 16 March 2017) at para 4.43.

13 The subsidiary proprietor's right to inspect and take copies of any document or record under s 47 of the BMSMA is not subject to any restrictions, whereas the data subject's access right under s 21 of the PDPA to access personal data about him is subject to restrictions. A subsidiary proprietor has the right to inspect and take copies of CCTV footage under s 47 of the BMSMA without any requirement for the redaction of personal data about other individuals that happen to be captured as part of the video record. If the same request is made by the subsidiary proprietor under s 21 of the PDPA in exercise of his data subject access rights, personal data of other individuals have to be redacted unless their consent has been obtained.

14 In the face of this inconsistency, I am obliged by s 4(6) of the PDPA to decide that s 47 of the BMSMA shall prevail over s 21 of the PDPA in the present case, to the extent that the Organisation can provide inspection of CCTV footage to the *subsidiary proprietor* without the need to redact personal data of other individuals or to seek their consent for such disclosure. However, it should be borne in mind that s 47 of the BMSMA only applies when it is a person entitled under that provision, *eg*, a *subsidiary proprietor*, making the application for inspection of the CCTV record. It has no application when the request for inspection is made by any other resident or visitor to the property, in which case the request should be handled as a data subject access request under s 21 of the PDPA.

15 This decision should be distinguished from *Re Exceltec Property Management Pte Ltd*[10] also a decision that involved s 47 of the BMSMA, where it was decided that information on the strata roll was generally available to the public by reason that the class of persons entitled to apply was broadly defined and *as a matter of fact* there were few or no restrictions imposed for a person to gain access to the strata roll: all an applicant was required to do was make an online application and pay the prescribed fee.[11] In the present case, there is no evidence that the CCTV video footage was broadly accessible in the same manner. The contrary was in fact true. Access in this case was restricted to a subsidiary proprietor and inspection was conducted in the presence of two other council members. *Re Exceltec*

10 [2018] PDP Digest 184.

11 *Re Exceltec Property Management Pte Ltd* [2018] PDP Digest 184 at [33] to [37].

Property Management Pte Ltd should not be interpreted in an overly broad manner to render all documents accessible under s 47 of the BMSMA to be publicly available. The analysis in *Re Exceltec Property Management* called for both a legal and a factual analysis. In order that CCTV footage do not become *de facto* publicly available, management corporations would do well to put in place policies and practices to ensure that only parties entitled to access under s 47 of the BMSMA are given access to CCTV footage.

CONCLUSION

16 For the reasons set out above, I am therefore of the view that the Organisation has not breached s 21 of the PDPA when it provided the subsidiary proprietor inspection of the CCTV footage under s 47 of the BMSMA.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Singapore Cricket Association and another

[2019] PDP Digest 270

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1704-B0707
Decision Citation: [2019] PDP Digest 270; [2018] SGPDPC 19

Openness Obligation *– Requirement to develop and implement policies and practices*
Protection Obligation *– Disclosure of personal data – Insufficient administrative security arrangements*

21 August 2018

BACKGROUND

1 This case concerns the unauthorised disclosure of the personal data of cricket players on the Singapore Cricket Association's ("SCA") websites (the "Incident"). On 20 April 2017, the Personal Data Protection Commission (the "Commission") received a complaint regarding the unauthorised disclosure of personal data on the player profile pages on the SCA's websites and commenced its investigations thereafter. The Deputy Commissioner's findings and grounds of decision based on the investigations carried out in this matter are set out below.

2 The SCA is the official governing body of the sport of cricket in Singapore. It administers various cricket leagues in Singapore with more than 100 cricket clubs participating across several league divisions. The SCA owns the rights to the domain name www.singaporecricket.org (the "First Domain"), which has served as the SCA's official website since August 2007 ("Website"). The SCA also owns the rights to the domain name, www.cricketsingapore.com ("Second Domain"). Both domains were accessible to the public and the hosting of both domains were set up and managed by the SCA or on its instructions.

3 All clubs and their players are required to register with the SCA in order to participate in any of the SCA leagues. To register new players, clubs are required to submit the following player personal data through the registration form on the SCA's Website:[1]

(a) player name;
(b) player photograph;
(c) NRIC/FIN number;
(d) date of birth;
(e) e-mail address; and
(f) mobile number.

4 Player profile pages which showed the registered player's name, photograph, player code (a unique identifier assigned to players upon registration) as well as player statistics ("Player Profile Information") have been made available on the SCA's Website since it was launched in August 2007. Player Profile Information was disclosed on the SCA's Website to identify players participating in the leagues and to promote interest in the sport by providing the public information on the league players in the same way that some football and tennis players have public profiles.[2]

5 In February 2016, the SCA engaged Massive Infinity Pte Ltd ("MI"), a Singapore-based web design and development company, to revamp its Website and design and develop a new custom web portal for the SCA ("Revamped Website") in accordance with the website development specifications provided to MI.[3] However, as the SCA's website development specifications were set out in very general terms and did not specify the contents of the Revamped Website, details of the exact contents of the

1 Clubs were also required to provide information such as the season, league, division and club the player will be playing in as well as the player's category, role, bowling style and batting style.

2 Given the Singapore Cricket Association's long-standing practice of publishing Player Profile Information on its Website, players were deemed to have consented to the disclosure of the Player Profile Information when they registered to participate in the league through their respective clubs.

3 Together with the Website revamp, the Singapore Cricket Association also switched the web hosting company for the First Domain from an India-based web hosting company to one in Singapore. However, Massive Infinity Pte Ltd was only engaged to provide the user interface design and web development of a new custom web portal and did not provide web hosting services.

Revamped Website were communicated to MI in meetings, and through phone calls and WhatsApp text messages.

6 During the development and testing of the Revamped Website, the Second Domain was used as a trial or user acceptance testing site.[4] In the course of conducting user acceptance tests, the SCA requested the inclusion of some additional pages to the Revamped Website, such as the player profile pages. These additional pages were not part of the original design and were therefore not included in the design documents. Neither party was able to produce any evidence of instructions from the SCA on the type of player information that was to be shown on the new player profile pages. While the SCA represented that its intention was for the Revamped Website to show the same Player Profile Information that was on its original Website, it conceded that it did not expressly highlight the type of player information that was to be included on the player profile pages on the Revamped Website.

7 In the absence of any specific instructions on the required fields for the new player profile pages, MI created the new player profile pages based on the information collected from the SCA's player registration page on the Website. Consequently, in addition to the Player Profile Information that had previously been disclosed on the Website, the new player profile pages included fields for personal data such as the player's NRIC/FIN number, date of birth, e-mail address and mobile number (the "Additional Player Personal Data").

8 During the investigations, the parties gave conflicting accounts as to when the SCA was first shown the new player profile pages. MI represented that before the new player profile pages with actual player data were pushed to the Second Domain, mock-up player profile pages created using

4 The Second Domain was removed by the Singapore Cricket Association ("SCA") on 17 April 2017 after the First Domain had stabilised. Massive Infinity Pte Ltd ("MI") had set up a staging environment (scastg.azurewebsites.net domain) ("Testing Domain") for development and testing purposes. The Testing Domain was the only web hosting setup maintained by MI for development purposes and was closed soon after the code was pushed to the SCA's testing environment, *ie*, the Second Domain, on 17 November 2016. The Testing Domain was not accessible by search engines.

"dummy data" were sent to the SCA for its review. The Revamped Website, including the new player profile pages with actual player data from the database of registered players' data that the SCA had provided to MI ("Registered Players Database"),[5] was pushed to the Second Domain for the SCA's review and approval on 17 November 2016. The SCA, however, represented that it had only discovered that contrary to its intention, the Additional Player Personal Data was disclosed after MI uploaded the new player profile pages on the Second Domain and subsequently on the First Domain.

9 The SCA and MI held a meeting on 28 November 2016 to review the changes that MI had made to the Revamped Website. However, the SCA claimed that at the time of the meeting, the new player profile pages were missing from the Revamped Website. MI, in turn, stated that as the SCA did not raise any issues with the new player profile pages at the meeting, MI assumed that the SCA had approved the content of the new player profile pages and they were to proceed to production as created.

10 The Additional Player Personal Data was made available on the First Domain on or around 9 January 2017 after the system was migrated from the staging server (*ie*, the Second Domain). Upon discovering that the Additional Player Personal Data was disclosed on the new player profile pages, the SCA took steps to remove them from the player profile pages, leaving only the Player Profile Information.

11 The Additional Player Personal Data was disclosed on the respective player profile pages and therefore publicly accessible for the following periods:

(a) from the Second Domain, from 17 November 2016 until its removal on 6 February 2017;
(b) from the First Domain, from around 9 January 2017 until its removal on 6 February 2017; and
(c) cached versions of the Revamped Website continued to be listed among the search results on major online search engines until the SCA submitted a request for their removal in May 2017.

5 The Singapore Cricket Association received the database of the registered players' personal data from its previous vendor based in India.

12 The parties were unable to determine conclusively the exact number of players whose personal data had been disclosed on the Revamped Website on the First and Second Domains. However, based on the number of pages cached by the search engines, the SCA estimated that as many as 100 players were affected.

FINDINGS AND BASIS FOR DETERMINATION

13 The main issues for determination are:

(a) whether MI breached s 24 of the Personal Data Protection Act 2012[6] ("PDPA");

(b) whether the SCA complied with its obligations under s 12(*a*) of the PDPA; and

(c) whether the SCA breached s 24 of the PDPA.

14 It was not disputed that the Player Profile Information and Additional Player Personal Data disclosed on the new player profile pages were "personal data" as defined in s 2(1) of the PDPA.

Whether Massive Infinity Pte Ltd breached section 24 of the Personal Data Protection Act

15 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. MI was engaged by the SCA to revamp the Website and was subsequently instructed to create new player profile pages on the Revamped Website. The SCA gave MI a copy of the SCA's Registered Players Database in order for MI to upload the players' personal data to the new player profile pages. Accordingly, the Deputy Commissioner is satisfied that the personal data in the Registered Players Database was in MI's possession or under its control at all material times and MI was required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

6 Act 26 of 2012.

16 However, MI intentionally disclosed the Additional Player Personal Data on the new player profile pages because it was under the impression that the SCA had intended for the Additional Player Personal Data to be disclosed on the new player profile pages. In this regard, seeing as MI relied on the SCA for directions as to the personal data that was to be disclosed on the player profile pages and there was no evidence that MI should have known what personal data was to be disclosed from the SCA's instructions or from the circumstances, the Deputy Commissioner finds that MI did not act in breach of its Protection Obligation under s 24 of the PDPA when it disclosed the Additional Player Personal Data.

Whether the Singapore Cricket Association complied with section 12(a) of the Personal Data Protection Act

17 Section 12(*a*) of the PDPA imposes an obligation on organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. The SCA represented, in a witness statement dated 12 June 2017 provided by a representative authorised by the SCA, that it did not have any internal guidelines and/or policies for the protection of personal data at the time of the Incident and that it was in the process of reviewing this and coming up with a data protection policy and guidelines.[7]

18 It bears repeating that the development and implementation of data protection policies is a fundamental and crucial starting point for organisations to meet their obligations under the PDPA.[8] As the Deputy Commissioner highlighted in *Re Aviva Ltd*[9] on the role of general data protection policies:

> Data protection policies and practices developed and implemented by an organisation in accordance with its obligations under s 12 of the PDPA are generally meant to increase awareness and ensure accountability of the organisation's obligations under the PDPA.

---

7 The Singapore Cricket Association had a data protection officer, but its data protection officer had not undergone any training on data protection matters.

8 *Re M Stars Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 at [25].

9 [2018] PDP Digest 245 at [32].

19 In this regard, the Deputy Commissioner agrees with the observations in the Joint Guidance Note issued by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia that employees will be able to better protect personal data when they are able to first recognise when a matter involves data protection:[10]

> Training and general education on privacy are very important. *Our Offices have seen instances where issues were not identified as privacy issues when they should have been. As a result, appropriate steps were not taken to prevent or address privacy breaches. In other cases, we have seen a lack of awareness or appreciation for privacy risks on the part of employees result in the development of products or services that were not compliant with applicable privacy law.* In Alberta, human error is the most common cause of reported breaches resulting in a real risk of significant harm to an individual. Examples include: misdirected faxes and mail, e-mail addresses viewable in mass e-mails, inappropriate disposal of documents, and disclosure of passwords.
>
> *Employees will be able to better protect privacy when they are able to recognize a matter as one that involves personal information protection.*
>
> [emphasis added]

20 Therefore, by the SCA's own admission, it failed to meet its obligations under s 12(*a*) of the PDPA.

Whether the Singapore Cricket Association complied with section 24 of the Personal Data Protection Act

21 The SCA obtained the Registered Players Database, which contained the personal data of all its registered players, from its previous vendor based in India. A copy of the Registered Players Database was handed over to MI "for a week" for MI to upload the players' data onto the new player profile pages. The SCA alone had the right to determine whether and how many of the players' personal data would be held and presented in the Revamped Website. Hence, the Deputy Commissioner is satisfied that the personal

---

10 Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, "Getting Accountability Right with a Privacy Management Program" (April 2012) at p 13.

data in the Registered Players Database remained under the SCA's control at all material times.

22 Having considered the matter, the Deputy Commissioner finds that the SCA failed to put in place reasonable security arrangements to protect the personal data in its control and therefore acted in breach of its Protection Obligation under s 24 of the PDPA.

23 Player profile pages were on the SCA's original Website and the SCA's eventual actions disclose its intention to retain player profile pages as a function of the Revamped Website. As stated in [5] above, the SCA did not provide sufficiently detailed requirements to MI. The omission of the player profile pages was eventually discovered during user acceptance testing. The SCA then requested that player profile pages be retained on the Revamped Website. Again, the SCA did not provide detailed requirements specifications and MI was left to devise player profile pages based on the information provided by players via the online registration form. Needless to say, this disclosed too much personal data.

24 Despite the fact that the inclusion of player profile pages had been made during the final stages of the project, the SCA failed to follow up to check that this function of the Revamped Website had been properly implemented. Such an omission is particularly egregious given its context and chronology. A flaw in the Revamped Website had been identified by the SCA and certain directions had been given to MI. One would expect that the natural behaviour of the owner of a website would be to ensure that identified flaws are properly fixed. The omission of the player profile pages and how this has been resolved by MI ought to have been in the SCA's consciousness. This betrays the SCA's lackadaisical attitude towards protection of the personal data of registered players and sets the context for the severity of its negligence which is examined below.

25 First, the SCA provided a database of all existing players in its Registered Players Database to MI. It should have clarified whether its intention was for all the personal data in the Registered Players Database to be displayed in the new player profile pages. The SCA simply assumed that MI would replicate the same fields in the previous player profile pages. As owner of the Revamped Website, the onus is on the SCA to give clear instructions to MI. As a result of the SCA's failure to state in clear terms the required fields to be created in the new player profile pages, the Additional

Player Personal Data of as many as 100 registered players were disclosed on the First and Second Domains.

26 Second, considering that the registered players' personal data would be disclosed in the new player profile pages, the SCA ought, at the very least, to have reviewed the new player profile pages before MI uploaded it to the First and Second Domains. Had the SCA done so, the disclosure of the Additional Player Personal Data could have been avoided. It bears repeating that this omission is especially egregious given the fact that the SCA had identified a flaw, which would have meant that this omission should have been in its consciousness, but it failed to follow up with ensuring that it had been properly addressed.

27 Simply assuming that MI would replicate the same fields in the previous player profile pages is a clear derogation of its protection obligation. The provision of proper and clear instructions to the designer and developer of a website that holds personal data can and should form part of the protection obligations of the organisation that owns it. In failing to do so, the SCA is in breach of the protection obligation. Further, as mentioned above, the Deputy Commissioner found that the SCA's website development specifications lacked website content details. As a result, instructions and details of the SCA's requirements were conveyed to MI piecemeal in meetings and through phone calls and WhatsApp text messages, which appears to have led to confusion and miscommunication between the parties as to the exact requirements for the Revamped Website.

28 Regardless of whether the SCA was shown the new player profile pages at the 28 November 2016 meeting or earlier, the Deputy Commissioner finds that at least between 28 November 2016 and 6 February 2017,[11] the SCA could have and ought to have discovered and prevented the unauthorised disclosure of the Additional Player Personal Data on the new player profile pages, but failed to do so. However, the SCA was unable to explain why it had failed to pick up on the unintended disclosure of the Additional Player Personal Data earlier or provide sufficient information on what arrangements or measures (if any) were implemented to review the changes made to the Website.

---

11 As mentioned above, the Singapore Cricket Association removed the Additional Player Personal Data from the First and Second Domains on 6 February 2017.

29 At this juncture, the Deputy Commissioner reiterates that organisations that engage service providers to process personal data on their behalf should clarify and properly document the nature and extent of service provided.

30 This was highlighted in *Re Smiling Orchid (S) Pte Ltd*[12] where the Commissioner emphasised the need for a clear meeting of minds as to the services the service provider has agreed to undertake:

> 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 engaged 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. [emphasis added]

31 Also, as highlighted in the *Guide on Building Websites for SMEs*,[13] organisations that engage IT vendors to develop and/or maintain their websites should ensure that their IT vendors are aware of the need for personal data protection:

> *Organisations should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms. The contract should also state clearly the responsibilities of the IT vendor with respect to the PDPA.* When discussing the scope of the outsourced work, organisations should consider whether the IT vendor's scope of work will include any of the following:
>
> - *Requiring that IT vendors consider how the personal data should be handled as part of the design and layout of the website.*
> - Planning and developing the website in a way that ensures that it does not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the Internet.

12 [2017] PDP Digest 133 at [51].

13 Revised 10 July 2018, at para 4.2.1.

- Requiring that IT vendors who provide hosting for the website should ensure that the servers and networks are securely configured and adequately protected against unauthorised access.
- …
- When engaging IT vendors to provide maintenance and/or administrative support for the website, requiring that any changes they make to the website do not contain vulnerabilities that could expose the personal data. Additionally, discussing whether they have technical and/or non-technical processes in place to prevent the personal data from being exposed accidentally or otherwise.

[emphasis added]

32 Therefore, in the light of the above, the Deputy Commissioner finds that the Organisation failed to make reasonable security arrangements to prevent unauthorised disclosure of the Additional Player Personal Data and is therefore in breach of s 24 of the PDPA.

DIRECTIONS

33 Having found that the SCA is in breach of ss 12(*a*) and 24 of the PDPA, the Deputy Commissioner is empowered under s 29 of the PDPA to give the SCA such directions as it deems fit to ensure compliance with the PDPA.

34 The Deputy Commissioner took into account the following factors in assessing the breach and determining the directions to be imposed:

Aggravating factors

(a) the personal data disclosed included the registered players' NRIC/FIN numbers;

Mitigating factors

(b) the SCA took prompt action to mitigate the impact of the breach by removing the Additional Player Personal Data from the player profile pages on the First and Second Domains soon after it discovered the Incident; and

(c) the SCA co-operated fully in the investigation.

35 Having considered all the relevant factors of this case, the Deputy Commissioner hereby directs the SCA:

(a) to develop and implement policies and practices that are necessary for the SCA to meet its obligations under the PDPA within 90 days from the date of this direction;

(b) to conduct personal data protection training for its employees to ensure that they are aware of, and will comply with the requirements of the PDPA when handling personal data within 90 days from the date of this direction; and

(c) to inform the office of the Commissioner of the completion of the above directions within seven days of implementation.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Dimsum Property Pte Ltd

[2019] PDP Digest 282

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1805-B2096
Decision Citation: [2019] PDP Digest 282; [2018] SGPDPC 20

Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

21 August 2018

BACKGROUND

1 The complaint concerns the failure to protect the personal data of individuals in the possession or under the control of Dimsum Property Pte Ltd (the "Organisation"). The Organisation operated a website www.snappyhouse.com.sg (the "Website"), providing a platform for homeowners to sell and rent out property directly to others.

2 The Complainant was a member of the public who had visited the Website. On 9 May 2018, the Complainant filed a complaint with the Personal Data Protection Commission (the "Commission") that images of identification documents were made publicly accessible on the Website through two Web directories (or folders):

(a) www.snappyhouse.com.sg\templates\bootstrap2-responsive\assets\images\avatar (the "Avatar Directory"); and
(b) www.snappyhouse.com.sg\templates\bootstrap2-responsive\assets\images\indentity (the "Identity Directory").

MATERIAL FACTS

3 The Avatar Directory contained images uploaded by registered users on the Website as their profile avatars. These images included photographs of individuals, and one even included a photograph of a user's passport.

The Organisation intimated that image of the passport may have been intentionally or erroneously uploaded by the user.

4 The Identity Directory contained images of identification documents uploaded by 30 registered users for verification purposes. The Organisation had been collecting and storing these documents in the folder since November 2015, until the Website was taken down on 24 May 2018.

5 In total, the personal data of 31 individuals were accessible to the public. The passport image in the Avatar Directory and the 30 identification documents in the Identity Directory disclosed personal data such as individuals' name, photograph, address, passport number, NRIC number, thumbprint, date of birth, place of birth, gender, nationality, and date of issue/expiry of passport.

6 The Organisation had engaged the services of an overseas vendor (the "Vendor") to design and develop the Website. The completed Website was delivered in November 2015. No personal data had been transferred to the Vendor for the development of the Website.

7 The Organisation subsequently hired its own in-house developers in November 2015. The in-house developers took over the development and administration of the Website in January 2016. However, there was no further update or development of the Website since July 2016, and users continued to register on the Website and use the Website's functions until March 2018. The Website was taken down by the Organisation on 24 May 2018 and is no longer accessible. The Organisation was unclear if the Identity Directory had been publicly accessible at the time when the Website was delivered by the Vendor or had been made publicly accessible by its own in-house developers.

8 The Organisation was in possession and control of the personal data that appeared on the Website. Section 24[1] of the Personal Data Protection Act 2012 ("PDPA") therefore required the Organisation to make reasonable security arrangements to protect the personal data, which included

1 Section 24 of the Personal Data Protection Act 2012 (Act 26 of 2012) requires organisations to protect personal data in their possession or under their control. They are required to make reasonable security arrangements against unauthorised access, collection, modification and other risks listed in s 24.

protecting against the risk of unauthorised access. Moreover, the protection obligation did not extend to the Vendor as the Vendor did not process any personal data on behalf of the Organisation and was not a data intermediary. The Organisation therefore retained full responsibility for the IT security of its website, and the personal data contained within.

FINDINGS AND BASIS FOR DETERMINATION

9 The issue was whether the Organisation had made reasonable security arrangements to protect the personal data of its customers that was in its possession and control. The Organisation admitted that it was unaware of the need to protect the personal data that it stored in the web directories. This, in turn, resulted in the Organisation's failure to implement reasonable security arrangements to protect the personal data it had collected and kept in the two web directories. The Organisation should have protected the personal data by implementing access controls to limit web access to the two web directories to authorised users.

CONCLUSION

10 In the light of the above, I find that the Organisation did not put in place reasonable security arrangements to the protect personal data in its possession or control against risk of unauthorised access. The Organisation is therefore in breach of s 24 of the PDPA. In assessing the appropriate enforcement action in this case, I took into account the following:

(a) the Organisation's prompt actions to remove the personal data from public access;
(b) the number of individuals affected;
(c) the impact of the breach; and
(d) the Organisation had ceased operations of the Website.

11 Having considered these factors, I have decided to issue a warning to the Organisation for the breach of its obligation under s 24 of the PDPA without any directions or financial penalty.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Jade E-Services Singapore Pte Ltd

[2019] PDP Digest 285

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1801-B1632
Decision Citation: [2019] PDP Digest 285; [2018] SGPDPC 21

Protection Obligation *– Disclosure of personal data – Failure to implement reasonable security arrangements*

11 September 2018

BACKGROUND

1 The complaint concerns the failure to protect the personal data of individuals in the possession or under the control of Jade E-Services Singapore Pte Ltd (the "Organisation"). The Organisation is in the online clothing retail business and operates the e-commerce fashion retail website www.zalora.sg (the "Website") in Singapore.

2 The Complainant was a customer of the Organisation. She filed her complaint with the Personal Data Protection Commission (the "Commission") on 30 January 2018. The Complainant said she logged into her user account on the Website and was shown the account subpages of another customer. She could see the other customer's name, contact number, birth date, e-mail address and residential address.

MATERIAL FACTS AND FINDING

3 This case concerns s 24[1] of the Personal Data Protection Act 2012 (the "PDPA"). The issue was whether the Organisation had made

1 Section 24 of the Personal Data Protection Act 2012 (Act 26 of 2012) requires organisations to protect personal data in their possession or under their control. They are required to make reasonable security arrangements

(*continued on next page*)

reasonable security arrangements to protect the personal data of its customers that was in its possession or under its control. The Organisation was in possession and control of the personal data in the user account subpages of its customers. Customers, such as the Complainant, could access their user accounts on the Website.

4 As bot traffic took up much of the Website's bandwidth, the Organisation introduced a bot manager service on 30 January 2018. The bot manager would identify whether a request for subpages of the Website was made by a bot. It would then serve identified bots with cached subpages having the same URL as the actual subpages requested, therefore saving bandwidth. If there were no cached subpages with the same URL, the bot manager served the requested subpages. However, it would cache the subpages visited to be served to subsequent bot requests. The cache was refreshed every 24 hours.

5 The bot manager had a setting that would have prevented user account subpages containing personal data from being cached if it had been applied (the "Setting"). The Organisation, however, did not consider the possibility that the bot manager might misidentify an actual user as a bot. It believed that if users had logged into the website with their username and passwords, the bot manager would not consider them as a bot, and therefore not cache their account subpages. As such, the Organisation did not apply the Setting.

6 In the present complaint, the bot manager misidentified a user who logged in with her password as a bot. It cached her account subpages, which contained her personal data. They were then served to the Complainant, who was also misidentified as a bot. The Organisation should not have taken the risk of allowing web subpages with personal data to be cached for display. It should have applied the Setting from the start, when introducing the bot manager, to protect its customers' personal data. Following the incident, the Organisation had, on 1 February 2018, applied the Setting to disable the caching of subpages containing personal data.

---

against unauthorised access, collection, modification and other risks listed in s 24.

CONCLUSION

7 I find on the facts above that the Organisation did not make reasonable security arrangements to protect the personal data of its customers. The Organisation is therefore in breach of s 24 of the PDPA. I took into account the number of affected individuals (estimated by the Organisation at 23), the type of personal data at risk of unauthorised access and the remedial action by the Organisation to prevent recurrence. I have decided to issue a warning to the Organisation for the breach of its obligation under s 24 of the PDPA as neither further directions nor a financial penalty is warranted in this case.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Galaxy Credit & Investments Pte Ltd

[2019] PDP Digest 288

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1803-B1886
Decision Citation: [2019] PDP Digest 288; [2018] SGPDPC 22

Protection Obligation *– Context of disclosure rendered personal data sensitive – Stronger controls needed to protect sensitive personal data*
Protection Obligation *– Disclosure of personal data – Mistaken identity*

25 September 2018

BACKGROUND

1 Is it appropriate for a licensed moneylender, or any organisation, to attach a photograph of a debtor to a letter demanding payment of a debt and leave both the photograph and letter at the residence of the debtor? What is the objective or purpose of such a practice? If the Organisation had considered these questions, the unauthorised disclosure in this matter may very well have not occurred.

2 The facts in this matter are straightforward and are not in dispute. On 16 March 2018, the Registry of Moneylenders & Pawnbrokers, Ministry of Law ("ROMP") informed the Personal Data Protection Commission (the "Commission") that the Organisation had sent three letters of demand, each with a photograph of a borrower, [redacted] (replaced with "Mr T"), to the residence of another borrower, [redacted] (replaced with "Mr W"). The Commission proceeded to investigate into an alleged breach of the Personal Data Protection Act 2012[1] ("PDPA").

1 Act 26 of 2012.

MATERIAL FACTS

3 The Organisation is a licensed moneylender. As part of its business, the Organisation issued letters of demand ("LODs") to borrowers who defaulted on the repayment of their loans. These LODs would be delivered to the defaulting borrowers by a third-party debt collector engaged by the Organisation. Prior to each delivery, the Organisation would provide its debt collector with the LOD and a photograph of the borrower. According to the Organisation, the purpose of providing a photograph was to help the debt collector correctly identify the borrower.

4 The Organisation instructed the debt collectors to attach the photograph to the LOD and hand it to the borrower. If the borrower was not present, the Organisation's instruction to the debt collector was to place the photograph together with the LOD into a sealed envelope and leave the sealed envelope at the borrower's residence.

5 To obtain photographs of all their borrowers, the Organisation took photographs of each new borrower when they visited the Organisation's premises to obtain the loans. These photographs were stored on the Organisation's system and only tagged to their respective borrowers' accounts at the end of each day.

6 Investigations revealed that Mr T and Mr W had both borrowed money from the Organisation on the same day, 17 October 2017. However, Mr W's photograph was not taken that day, and the Organisation's staff had incorrectly tagged Mr T's photograph to Mr W's account.

7 Mr W defaulted on his payment for the loan he had taken out and the Organisation issued three LODs, dated 1, 5 and 9 February 2018, to Mr W. The assigned debt collector left all of them at Mr W's residence as Mr W was not present when the debt collector visited him on those dates. As a result of the incorrect tagging, Mr T's photograph was attached to all three LODs. Mr T's photograph did not include any other identifying information. The Organisation was only made aware of the alleged data breach upon notification by ROMP.

8 Following the incident, the Organisation explained to the Commission that the incident involved a human error on its part. It attempted to recover the wrongly attached photograph of Mr T, but was

unable to locate or contact Mr W. It subsequently informed the Commission that the following remedial actions were taken:

(a) The Organisation changed its practice of tagging photographs such that all photographs of new borrowers would be tagged immediately to ensure that each photograph had been taken and tagged correctly.

(b) The Organisation changed its practices relating to the use of the borrowers' photographs for debt collection. First, the photograph would no longer be attached to the LOD and handed to the borrower or left at the borrower's residence. Second, the debt collector would be handed a copy of the photograph for identification purposes, but the photograph would be returned to the Organisation for shredding after each LOD was delivered. Third, a new photograph would be generated for the debt collector if a subsequent trip to the same borrower's residence was required.

(c) The Organisation was looking into providing more data protection training for its employees.

(d) The Organisation also informed and reminded all of its employees to follow the relevant guidelines recommended by the Commission.

FINDINGS AND BASIS FOR DETERMINATION

9 The issues to be determined are as follows:

(a) whether the Organisation had complied with its obligations under s 24 of the PDPA; and

(b) whether the Organisation was in breach of s 18(*a*) of the PDPA.

10 As a preliminary point, it was not disputed that the photographs of the Organisation's borrowers fell within the definition of "personal data" under s 2(1) of the PDPA as it was clearly possible to identify the borrowers from that data and, in fact, that was the Organisation's intention in collecting the photographs of borrowers. Further, the *Advisory Guidelines on*

Key Concepts in the Personal Data Protection Act[2] consider photographs with a facial image of an individual as personal data.

11 The Deputy Commissioner also found that the Organisation had not breached its consent obligation. Notably, the Organisation's collection of its borrowers' photographs for the purpose of debt recovery did not require consent as it fell within the exception in para 1(*i*) of the Second Schedule to the PDPA. In any case, the Organisation had obtained consent from its borrowers before taking their photographs. It had also obtained consent from the borrowers, as part of their contract, to "release all or some of [their] personal/loan/contract details to [third party organisations] for the purpose of … debt recovery". It was therefore not in breach of its consent and notification of purpose obligations under ss 13 and 20 of the PDPA.

Whether the Organisation had complied with its obligations under section 24 of the Personal Data Protection Act

12 Section 24 of the PDPA requires an organisation to protect the 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 (the "Protection Obligation").

13 The Deputy Commissioner finds that the Organisation did not have adequate measures in place to ensure that the borrowers' photographs were correctly tagged to their respective accounts. Its practice of tagging the borrowers' photographs at the end of each day instead of immediately tagging the photographs when they were taken created an obvious vulnerability; this arrangement was susceptible to errors being made in the tagging of photographs. To this end, the mistagging of Mr T's photograph could have been prevented if the Organisation had immediately tagged photographs to the account of the respective borrowers once the photographs were taken. This would have clearly reduced the possibility of incorrect tagging.

14 As such, the Deputy Commissioner finds that the Organisation had failed to make reasonable security arrangements to protect the personal data

2 Revised 27 July 2017, at para 5.10.

in its possession and within its control. The Organisation is, therefore, in breach of s 24 of the PDPA.

Whether the Organisation had used the personal data for a purpose that a reasonable person would consider appropriate in the circumstances

15 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. As observed in *Re AIA Singapore Private Limited*[3] at [18]:

> 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 …

16 Despite the fact that Organisation had obtained consent for use of its borrowers' personal data for the purposes of debt collection, the issue before the Deputy Commissioner was whether the use of the borrower's photograph, by placing it together with an LOD in a sealed envelope and leaving it at his or her residence, was a usage of personal data that a reasonable person would consider appropriate in the circumstances.

17 In our earlier decision of *Re Credit Counselling Singapore*,[4] the Commissioner considered the financial information of an individual, which includes information of the individual's indebtedness, to be "sensitive personal data" (at [15]). In particular, the Commissioner explained that:[5]

> Disclosure of an individual's indebtedness to other third parties could lead to harm to the individual because it could result in social stigma, discrimination or tarnish his reputation. These are real possibilities that can affect a person's life. Hence the confidentiality of the individual's financial information should not be treated lightly.

A similar position has also been adopted by foreign data protection authorities in the UK, Canada and Hong Kong. The point to be reiterated

---

3 [2017] PDP Digest 73.

4 [2018] PDP Digest 295.

5 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [19].

here is that organisations who have access to such personal data, such as licensed moneylenders, should exercise a greater degree of diligence and care in the handling and use of such personal data.

18 The Organisation explained that the purpose of handing the photograph to the debt collector was so that the debt collector could identify the borrower before serving the LOD. However, it did not provide an explanation for its practice of placing the borrower's photograph together with the LOD and handing it over to the borrower or leaving it at the borrower's residence.

19 In determining whether the use of personal data is for a purpose that would be considered appropriate by a reasonable person, the Deputy Commissioner would consider the purpose of such use as expressed by the Organisation. However, given that the Organisation had failed to address the purpose of placing the borrower's photograph together with the LOD and leaving it at the residence of the borrower, even though the Organisation was asked, the Deputy Commissioner draws the inference that there was no appropriate purpose for using the borrower's photographs in such a manner. Further, there is no obvious reason for this practice. As such, the Deputy Commissioner finds that the practice of placing a borrower's photograph together with an LOD in an envelope and leaving it at the borrower's residence is not for a purpose that a reasonable person would consider appropriate in the circumstances of this matter and is therefore a breach of s 18(*a*) of the PDPA. The Organisation should have exercised greater care in handling this sensitive personal data and used it only where appropriate.

DIRECTIONS

20 Having found that the Organisation is in breach of ss 18(*a*) and 24 of the PDPA, the Deputy Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

21 In assessing the breach and determining the directions to be imposed on the Organisation, the Deputy Commissioner took into account the following factors:

(a) the personal data disclosed in the data breach comprised a photograph of Mr T, which was sensitive personal data as it

indicated that Mr T was an existing borrower of the Organisation;

(b) the unauthorised disclosure had been to a single third party;

(c) no other complaints of the photograph disclosed being misused have been received hitherto;

(d) the risk of substantive loss or damage is low having regard to the fact that no further documentation of Mr T was attached to the photograph;

(e) while attaching the photograph to the LOD and leaving it at the residence was an inappropriate use of personal data, its effect was minimal since it was placed in a sealed envelope and not publicly displayed;

(f) the Organisation had since stopped the practice of attaching the borrower's photograph to the LOD; and

(g) the Organisation had undertaken measures proactively and swiftly to improve on its processes to prevent a recurrence of the incident.

22 In view of the factors noted above, the Deputy Commissioner has decided not to issue any direction to the Organisation to take remedial action or to pay a financial penalty. Instead, the Deputy Commissioner has decided to issue a warning to the Organisation for the breach of its obligations under ss 18(*a*) and 24 of the PDPA.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re GrabCar Pte Ltd

[2019] PDP Digest 295

Coram: Tan Kiat How, Commissioner
Case Number: DP-1706-B0871
Decision Citation: [2019] PDP Digest 295; [2018] SGPDPC 23

Personal data *– Business contact information*
Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

27 September 2018

BACKGROUND

1 This case involves the unauthorised disclosure of the personal data of GrabHitch drivers in a Google Forms survey created by the Organisation that was accessible online (the "Incident"). The Personal Data Protection Commission (the "Commission") received a complaint from one of the drivers whose personal data was disclosed in the Incident and commenced its investigations thereafter. The Commissioner set out below his findings and grounds of decision based on the investigations carried out in this matter.

MATERIAL FACTS

2 The Organisation was incorporated in September 2014 and has been providing the GrabHitch service since November 2015. GrabHitch is a paid carpooling service operated by the Organisation that matches individual non-commercial private car owners ("Hitch Drivers") with people who are commuting along the same route.[1] Hitch Drivers are

1 Individuals who provide carpool trips that adhere strictly to the conditions set out in the Road Traffic (Car Pools) (Exemption) Order 2015 (S 94/2015) are
(*continued on next page*)

permitted to charge a fare to cover the Hitch Driver's variable costs, such as petrol and car depreciation based on the distance of the ride.

3 In accordance with the Organisation's Driver's Code of Conduct, Hitch Drivers who fail to comply with the terms and conditions or code of conduct may be penalised through account deactivation, the withholding, reduction or forfeit of driver incentives or credits, suspension or permanent banning. Conduct that would warrant a suspension of a Hitch Driver's account includes fraud; booking and cancellation offences; offences concerning fares and payments; and passenger experience, safety or security offences such as harassment.

4 At the time of the Incident, the Organisation had suspended the accounts of 20 Hitch Drivers for various offences such as unacceptable behaviour and/or usage of the platform; these Hitch Drivers had appealed against their suspensions. Of these 20 Hitch Drivers, two of them were also GrabCar drivers. The Organisation created the "GrabHitch SG Appeal Form" using Google Forms, to allow the Hitch Drivers to submit an appeal to the Organisation and for the Organisation to contact them for further investigation.

5 Hitch Drivers whose accounts had been suspended were able to access the Google Form on 16 June 2017 at 10.00am. They were required to fill up the following fields in the Google Form ("Appeal Form Data") if they wanted to submit an appeal to the Organisation:

(a) name as per NRIC;
(b) NRIC number;
(c) mobile number;
(d) vehicle plate number; and
(e) appeal statement to explain their case for appeal including reasons to justify the reactivation of their account.

6 The Incident was the first time that the Organisation used Google Forms for the purposes of collecting responses in respect of appeals. Its intention was to allow its employees to access and review the Appeal Form Data to review suspensions. However, the employee who was responsible

---

exempt from the certain requirements under the Road Traffic Act (Cap 276, 2004 Rev Ed), such as the requirement to obtain the appropriate commercial licences and insurance.

for uploading the Google Form had chosen the incorrect setting by selecting the setting "Respondents can: See summary charts and text responses". As a result, all Hitch Drivers who had submitted the Google Form to appeal against their suspensions were able to view all the Appeal Form Data contained in the responses, both their own as well as the other Hitch Drivers who had appealed. Investigations disclosed that only the Hitch Drivers and the Organisation's employees were able to access the Appeal Form Data.

7 After being notified of the Incident, the Organisation promptly removed the ability of Hitch Drivers to access the Appeal Form Data. The total duration that the Google Form was in use was less than eight hours; the Appeal Form Data was uploaded on the same morning that the complaint was received and access to the data by Hitch Drivers was removed by 5pm the same day.

FINDINGS AND BASIS FOR DETERMINATION

8 The issues for determination are:

(a) whether the information disclosed constituted personal data; and

(b) whether the Organisation breached s 24 of the Personal Data Protection Act 2012[2] ("PDPA").

9 Even though it was an employee of the Organisation who had uploaded the Google Form with the wrong settings, under s 53(1) of the PDPA, any act done or conduct engaged in by a person 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 by him, regardless of whether it was done or engaged in with the employer's knowledge or approval. The Organisation is therefore responsible for its employee's conduct in relation to the Incident.

Whether the information disclosed constituted personal data

10 In this case, given that individual Hitch Drivers can be identified from the Appeal Form Data which was disclosed in the Incident

2 Act 26 of 2012.

(specifically, the Hitch Drivers' names, mobile phone numbers, NRIC numbers, vehicle plate numbers as well as their appeal statements), the Appeal Form Data is personal data as defined in the PDPA. In this regard, the Organisation is required to comply with the data protection obligations under the PDPA in respect of the Appeal Form Data.

11 Also, the Organisation in its representations dated 14 May 2018 indicated that the suspensions or bans were in relation to Hitch Drivers allegedly either exceeding the statutorily allowed number of trips per day or to "game" the system. The Organisation had subsequently, on 1 June 2018, in response to a question from the Commission on why the Organisation treated such transgressions as worthy of a suspension, stated that:

> We take gaming very seriously as it affects the integrity of our service offerings. Also, it is against our driver Code of Conduct: https://www.grab.com/sg/driver/hitch/code-of-conduct/. I draw your attention to the following clauses:
>
> Provide an honest service. Any form of cheating (e.g. Failure to return the full balance to passengers or requesting for full payments during promotional periods) or suspected fraudulent activity is prohibited and will trigger further investigation from the Company, as we reserve the right to ensure all transactions are genuine.
>
> The Company maintains a zero-tolerance policy regarding all infringements and violations of this Code of Conduct and the Driver acknowledges that this may result in suspension or termination of user access to the Grab platform

12 It is therefore the Organisation's case that a driver who "games" the system exhibits a lack of probity suggestive of fraudulent intent. These are serious allegations and the Organisation ought to have treated such personal data with the appropriate care in the knowledge that the unauthorised disclosure of the Appeal Form Data would result in such serious allegations being disclosed as well.

13 As noted at [4] above, two out of the 20 Hitch Drivers are also drivers of GrabCar. In this regard, unlike GrabHitch, which is a non-commercial social carpooling service, GrabCar is a private-hire car service that allows passengers to book a chauffeured ride for a fee and can only be provided by vehicles and drivers with the appropriate commercial licences. There is therefore the additional consideration that, pursuant to s 4(5) of the PDPA, the data protection obligations do not apply to business contact information of these two GrabCar drivers. (Business contact information is

defined to be 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.)

14 In *Re Comfort Transportation Pte Ltd*[3] ("*Comfort Transportation*") (at [9]), the Commissioner found that taxi drivers' mobile phone numbers that were used for, or related to, their business as taxi drivers fell within the definition of "business contact information" because, among other things, the organisation disclosed the taxi drivers' mobile phone numbers to passengers as a means for them to contact the taxi driver after a booking has been made. Thus, the name and mobile phone numbers provided by the two GrabCar drivers who were also Hitch Drivers are considered business contact information. The vehicle plate number is not business contact information since this is a means of *identification of the vehicle* that was used to provide the commercial GrabCar service and the driver of the said vehicle, but not a means of *contacting the driver*. That said, their NRIC numbers would not fall within the definition of business contact information.

Whether the Organisation breached section 24 of the Personal Data Protection Act

15 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Organisation represented that it uses the Single Sign-On authentication process with Google's suite of authentication services to protect access to the Appeal Form Data. Access to the Appeal Form Data is accessible only to intended individuals through individual file-sharing permissions.

16 However, as mentioned above, the Incident had occurred because the employee responsible for uploading the Google Form had chosen the incorrect setting "Respondents can: See summary charts and text responses". At the time of the Incident, the Organisation did not have any policies or procedures to guide its employees regarding the use of Google

3 [2017] PDP Digest 122.

Forms to collect personal data nor did it provide any training. Following from the Incident, the Organisation represented in its response to the first Notice to Produce dated 11 July 2017 that it was in the midst of preparing documents to better guide its employees on the use of Google Forms to prevent a similar occurrence in the future.

17 The Incident was the first time that Google Forms were used for the purposes of collecting responses (including the Hitch Drivers' personal data) in respect of appeals. Since there are easily accessible introductory articles such as the Google support article "What can you do with Forms?",[4] the onus is on the Organisation to ensure that it had a sufficient understanding and appreciation of the product before making use of it, particularly where it will be used to collect, use and/or disclose personal data.

18 This is a position that was taken in *Re GMM Technoworld Pte Ltd*[5] ("*GMM Technoworld*"). In that case, the Organisation created an online warranty registration form using a third party paid plug-in for Wordpress which allowed for the capture of personal data on the website. However, as a result of the Organisation's misunderstanding and incorrect use of the functions of the plug-in, the personal data of approximately 190 of its customers were displayed on its website.

19 As observed in *GMM Technoworld* (at [12]):

> … the Formidable Forms website had webpages 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

4 See "What Can You Do With Forms?" *G Suite Learning Center* <https://gsuite.google.com/learning-center/products/forms/get-started/#!/> (accessed 18 April 2019).

5 [2017] PDP Digest 128.

> 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 to the collection of personal data, and without ensuring that the plug-in (if properly configured) adequately protects the organisation's personal data.* [emphasis added]

20 In the light of the absence of any security arrangements to protect personal data from such unauthorised disclosure, the Commissioner finds that the Organisation has contravened s 24 of the PDPA.

DIRECTIONS

21 Having found the Organisation to be in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

22 In assessing the breach and determining the directions to be imposed, the Commissioner noted that the Appeal Form Data disclosed included the appeal statements which contained information about an individual driver's suspension from the GrabHitch service. The Organisation has indicated that these suspensions were on the basis that the drivers were "gaming the system". In the Organisation's own view, such "gaming of the system" suggested a lack of probity on the part of the drivers. Such allegations could potentially cause actual or potential harm, injury or hardship, including reputational damage where disclosed without authorisation. Also, the personal data disclosed included Hitch Drivers' NRIC numbers. The aforesaid was treated as an aggravating factor.

23 The Commissioner also took into account the following mitigating factors:

(a) the personal data was only disclosed to a limited number of individuals;

(b) the Organisation took prompt action to mitigate the impact of the breach by removing access to the Google Form within the same day that the Google Form was made available to the drivers. As such, the personal data was only disclosed for around seven hours;

(c) the Organisation had co-operated fully with the investigation; and

(d) the Organisation had notified the Commission of the Incident, albeit after the Commission had received a complaint from one of the affected Hitch Drivers.

24 The Commissioner has also considered the representations made by the Organisation through its letter of 14 May 2018. The Organisation's representations were as follows:

(a) To reconsider the position that the Organisation did not have the relevant data protection policies in place. In this regard, when the Organisation was asked for copies of its policies and internal guidelines for the protection of personal data which were valid as at the time of the Incident, the Organisation replied that it was in the process of drafting the relevant standard operating procedures ("SOPs"). In its representations, the Organisation clarified that it did in fact have relevant data protection policies in place and that the reference to the SOPs was in fact an updated version of its data protection policies. The Commissioner has considered the evidence provided and accepts that the Organisation did in fact have in place a data protection policy at the time of the Incident.

(b) The Hitch Drivers' appeal cases did not involve allegations of safety or security offences and instead involved exceeding the allowed two trips per day or "gaming" the system and that this type of case was much less sensitive than the facts in *Re Credit Counselling Singapore*.[6] The Commissioner had already taken this point into consideration in determining the quantum of the financial penalty.

25 The Commissioner, after reviewing the Organisation's representations as a whole, agreed to the Organisation's request for a reduction in the financial penalty initially proposed.

26 Having considered all the relevant factors of this case and the representations made by the Organisation as summarised above,

6 [2018] PDP Digest 295.

the Commissioner hereby issues a direction to the Organisation to pay a financial penalty of $6,000.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Club the Chambers

[2019] PDP Digest 304

Coram: Tan Kiat How, Commissioner
Case Number: DP-1701-B0439
Decision Citation: [2019] PDP Digest 304; [2018] SGPDPC 24

Protection Obligation *– Context of disclosure rendered personal data sensitive – Stronger controls needed to protect sensitive personal data*

4 October 2018

BACKGROUND

1 The Organisation had displayed A4-size notices comprising photocopies of the identity documents of 11 individuals whom the Organisation had banned from entry, along with descriptions of why those individuals had been banned. It is clearly well within the prerogative of an organisation to ban individuals from entry into its premises as a consequence of flouting its rules, in particular where the actions of such individuals affect the organisation's ability to maintain order and prevent criminal and other undesirable activities from being carried out. The question with which the Commissioner is concerned is whether the flouting of rules by individuals provides an organisation with carte blanche to treat the personal data of those individuals in any manner it sees fit. The Commissioner's findings and grounds of decision are set out below.

MATERIAL FACTS

2 The Organisation operates several gaming centres, or clubs, where members use computers connected by a Local Area Network ("LAN") to play multi-player games. The LAN gaming centre in question was the Organisation's Hougang branch (the "LAN shop").

3 To play at the LAN Shop, an individual must first sign up to become a member. All members are subject to the Organisation's rules and regulations. These rules stipulate that members who engage in prohibited behaviour, *eg*, online gambling, viewing of pornography, theft and truancy, will be banned from entry. According to the Organisation, the rationale for banning members is to maintain order and to prevent criminal and other undesirable activities from being carried out on the Organisation's premises.

4 On 11 January 2017, the Personal Data Protection Commission ("PDPC"), acting on a tip-off published in an online news report,[1] inspected the LAN Shop and found that the Organisation had posted notices ("Notices") comprising enlarged photocopies of the identity documents (*eg*, student pass, employment pass, Singapore Armed Forces identity card) of 11 individuals whom the Organisation had banned from entry into its premises. Each Notice contained personal data of a member who was banned.

5 The Notices disclosed different types of personal data, including a member's name, photograph, NRIC number/FIN, student identification number, mobile phone number, and name of employer, occupation, and remarks about a member ("remarks"). The Organisation provided these remarks to explain why the members had been banned from the LAN Shop, which included the following:

(a) "Banned for skipping classes and being very rude to his parents";
(b) "Banned for surfing pornography";
(c) "Banned for using others' Ezlink card";
(d) "Banned for stealing money and captured by CCTV";
(e) "Caught for stealing iPhone"; and
(f) "Caught online gambling during routine checks by police and arrested inside the centre".

6 The personal data in question, except for the remarks, had been collected at the time of application when the individuals filled up membership forms. The Organisation's stated intention for displaying the Notices is for the purpose of helping its staff identify members who had

1 Belmont Lay, "Gaming shop resorts to shaming misbehaving kids, but giving away too much personal info" *Mothership* (30 December 2016) <http://mothership.sg/2016/12/gaming-shop-resorts-to-shaming-misbehaving-kids-but-giving-away-too-much-personal-info/> (accessed 12 April 2019).

been banned from the LAN Shop. The staff will deny entry to the LAN Shop to banned members.

7 The sole proprietor of the Organisation alleged that he had instructed his staff to remove the Notices prior to 2 July 2014 when the data protection provisions of the Personal Data Protection Act 2012[2] ("PDPA") came into effect. However, the Notices continued to be displayed in the LAN Shop until they were finally taken down sometime between 11 January 2017 and 26 January 2017.

8 At the material time, the Organisation did not have in place any personal data protection policies or internal guidelines, although it claimed it had appointed a data protection officer.

FINDINGS AND BASIS FOR DETERMINATION

Two issues for determination

9 The relevant issues for determination in this case are:

(a) whether the Organisation obtained consent from its customers to disclose the personal data found in the Notices pursuant to s 13 of the PDPA;

(b) whether the disclosure of personal data was for a purpose that a reasonable person would consider appropriate in the circumstances pursuant to s 18(*a*) of the PDPA; and

(c) whether the Organisation developed and implemented the necessary data protection policies and practices pursuant to s 12(*a*) of the PDPA.

Whether the Organisation obtained consent from its customers to disclose the personal data found in the Notices

10 The Commissioner finds that the Organisation failed to obtain consent from its customers who were the subject of the Notices. The Commissioner's explanation of this finding is set out in greater detail below at [17] to [21] in discussing the Organisation's s 18(*a*) obligations.

2 Act 26 of 2012.

Whether the disclosure of personal data of its members was for a purpose that a reasonable person would consider appropriate in the circumstances pursuant to section 18(a) of the Personal Data Protection Act

11 Pursuant to s 18(*a*) of the PDPA, 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. Where the purpose of collection, use or disclosure does not fall within one of the excepted general purposes set forth in the Second, Third and Fourth Schedules, the purpose has to be both appropriate and also notified to the individual. Where the general purpose of collection, use or disclosure falls within one of the aforementioned exceptions, the specific purpose must still be reasonably appropriate, although there is no need to notify the individual subject to s 20(4) of the PDPA.

12 As a preliminary point, it was not disputed that the data contained in the Notices, which included details such as the banned member's name, photograph, NRIC number/FIN, student identification number, name of employer and occupation, fell within the definition of "personal data" under s 2(1) of the PDPA as it was possible to identity the 11 banned members from such details when taken as a whole. Also, given that the reason for the ban set out in each of the Notices was stated below the copy of the NRIC of each banned member, these reasons would also constitute personal data of the member. It was also not disputed that the personal data of the banned members was in the Organisation's possession and under its control at the material time.

13 Based on the investigations, the Commissioner finds that the purpose of disclosure of the 11 banned members' personal data was for an inappropriate purpose that breaches s 18(*a*) of the PDPA. The reasons for this finding are set out below.

Purpose of the Notices was to assist staff in identifying banned members and to inform banned members that they were prohibited entry into the LAN Shop

14 The sole proprietor of the Organisation, in his statement, made clear that the purpose for the display of the Notices was to assist staff in identifying banned members and to inform banned members that they were prohibited entry into the LAN Shop and the reason(s) for the ban.

15 In answer to the question "[p]lease state the purpose of the collection, use and disclosure of the personal data of those individuals", the sole proprietor stated, *inter alia*, that:[3]

> The purpose of collection, use and disclosure was to facilitate the application of membership and the provision of LAN gaming services to members which includes maintaining the rules and regulations.
>
> The rules and regulations such as banning members from entry due to surfing porn, online gambling or skipping schools (*sic*) is necessary to maintain order and prevent criminal activities from occurring in our premises. In fact, the aforesaid was encouraged by undercover police officers when they arrested people for online gambling.
>
> *Accordingly, we put the Notices to inform our staff and also those members banned from our clubs that they are prohibited entry.* Members never challenged or demanded us to bring down the Notices, but asked us for reasons. For example, a student will be informed that he has been banned because he skipped school. In this regard, some parents who complain to us for allowing their children to play in the LAN gaming shop will give permission for us to put the personal data of their children up to shame them so they will not do it again, but other parents will refuse.
>
> As for adults, some will ask us why we put up the Notices, and we will inform them that they have been caught by the police for online gambling.
>
> The students and adults need to show to us why we should remove the ban and Notices. For example, a student needs to show us good results. Likewise, the adult needs to show us that he did not commit the offence like surfing porn or online gambling, or only given a warning by the police.
>
> At the end of the day, CTC did not disclose the personal data with ill intent but rather to adhere to the laws and ensure our members comply with the laws as well. That said, *I admitted that we did post the Notices up and there were better ways to inform our employees and members of the ban.*
>
> [emphasis added]

16 From the above, it appears that the Organisation encountered situations where members were potentially using their premises for criminal activities such as online gambling or were playing truant and were in the LAN Shop when they were meant to be in school. To manage this, the Organisation decided to ban members who were suspected of committing an offence or undertaking any undesirable activities in their premises or

3 Witness Statement dated 3 February 2017.

playing truant. The purpose of the Notices was to inform the Organisation's staff which members were banned and to inform banned members of their ban and the reasons for the ban. Whilst the intentions are laudable, the modality of execution fell short.

17 At this juncture, the Commissioner would like to deal with the Organisation's claim that "some parents … will give permission for us to put the personal data of their children up …". The first point to take note of here is that the Organisation does not claim that consent was obtained from all its members who were the subject of the Notices which were displayed. In fact, this is an admission that consent to display the Notices was not obtained from all of the members who were the subject of the Notices. Even with respect to the claims made that consent was obtained in some of the cases, the Organisation failed to adduce any evidence of having obtained any such consent to support this claim other than the bare assertion made by the sole-proprietor of the Organisation.

18 The other point that the Commissioner would like to deal with as a preliminary issue is the claim that "[m]embers never challenged or demanded us to bring down the Notices". It should be noted that the failure to challenge or demand that the Notices be removed does not indicate that the member has unequivocally consented to the display of the Notices. The Organisation is required to either specifically obtain consent from the member to display the Notice or rely on deemed consent. The facts of this case, as uncovered during the investigations, do not lend themselves to a finding that members are deemed to have consented to the display of the Notices.

19 In this regard, given that the purpose of the Notices was limited to assisting staff in identifying and informing banned members that they were prohibited entry into the LAN Shop and the reason(s) for the ban, a reasonable person would not consider it appropriate to display the Notices to everyone who enters the LAN Shop. In fact, even the sole proprietor of the Organisation admits that other better ways existed to inform staff and banned members of the ban. Clearly, a simple way of doing so would have been to maintain an internal blacklist that only the staff on duty would be able to consult.

20 Given the above, it is telling that the sole proprietor instructed his staff to remove all the Notices before the PDPA came into effect. In this regard, the sole proprietor in his witness statement, in answer to the

question "[p]lease state whether CTC (*ie*, the Organisation) had taken any measures as of 30 December 2016 to prevent its employees to (*sic*) collect, use and disclose personal data without consent and notification. If so, please provide details of the measures taken", stated that:

> I actually instructed my employees to take down those the (sic) Notices before the Personal Data Protection Act came into effect. But I do not visit the clubs (including the LAN Gaming Shop) regularly so I was not able to monitor whether they did in fact take down the Notices.
>
> However, they took down the Notices before I received your notice to produce but I could (sic) not remember the date. They took it down during the Chinese new Year.

21 In the final analysis, the Organisation's intention to withhold its services from certain categories of users cannot be faulted nor should personal data protection laws impede such intentions. However, the manner in which it had carried out this purpose left much to be desired. The use of personal data to maintain an internal blacklist of customers that are banned from the cybercafe is an appropriate purpose. Section 18 of the PDPA requires that customers be notified of such use, and this could easily have been achieved with clear notification that some of the personal information provided by customers of the cybercafe during registration may be used for the purpose of managing the ongoing customer relationship, including the provision or suspension of services due to the customer's breach of the Organisation's rules. This would be an eminently appropriate purpose and, once notified, there would have been consent if the customer continues to make use of the cybercafe's facilities and services. One further point to highlight is that not all personal data disclosed in the Notices is required to achieve this purpose; photocopies of NRIC and FIN cards in particular need not have been used to achieve the stated purpose.

22 The manner of disclosure also left much to be desired. As the owner of the Organisation well knows, the blacklist need not be publicly displayed but can be kept as an internal list. The placement of the Notices also detracts from the stated purpose of assisting staff in the identification of *persona non grata*. These Notices were placed on the wall behind the counter such that when a member of staff is engaging with a customer, the Notices will be behind him. This detracts from its effectiveness as a blacklist for staff but suggests that it was intended to name and shame customers.

Whether the Organisation developed and implemented the necessary data protection policies and practices pursuant to section 12(a) of the Personal Data Protection Act

23 Section 12(*a*) of the PDPA provides that an organisation shall develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA.

24 In the present case, the Organisation admitted to the PDPC that, at the material time, it did not have in place any personal data protection policies or practices, or even internal guidelines with respect to personal data. As such, the Organisation was in breach of s 12(*a*) of the PDPA.

THE COMMISSIONER'S DIRECTIONS

25 Given the Commissioner's findings that the Organisation is in breach of its obligations under s 13, or in the alternative ss 18 and 12(*a*) of the PDPA, the Commissioner 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 S$1m.

26 In assessing the breach and determining the directions to be made, the Commissioner took into account, as an aggravating factor, the actual or potential harm that was posed to the 11 banned members due to the sensitive nature of the personal data disclosed.

27 The Commissioner also took into account the following mitigating factors:

(a) the Organisation was co-operative during investigations and the sole director of the Organisation delayed his overseas business trip in order to give his witness statement to the PDPC;

(b) the Organisation did not have malicious intentions in disclosing the personal data and had only displayed the Notices to maintain order in the LAN Shop and discourage criminal and undesirable activities from being carried out on its premises; and

(c) the Organisation took prompt remedial action to remove the Notices before the PDPC sent it a Notice to Produce Documents and Information.

28 Having carefully considered all the relevant factors noted above, pursuant to s 29(2) of the PDPA, the Commissioner hereby directs that the Organisation to:

(a) comply with s 12(*a*) of the PDPA by developing and implementing policies and practices that are necessary for the Organisation to meet the data protection provisions of the PDPA within 60 days of the date of the Commissioner's direction; and

(b) pay a financial penalty of S$7,000 in accordance with the Commissioner's direction, failing which interest at the rate specified in the Rules of Court[4] in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

4 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Big Bubble Centre Pte Ltd

[2019] PDP Digest 313

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1802-B1770
Decision Citation: [2019] PDP Digest 313; [2018] SGPDPC 25

Disclosure of personal data – *Consent obligation*

28 November 2018

1 The circumstances which led to the complaint over Big Bubble Centre's (the "Organisation") actions is a common one in today's social media age. It usually starts with a dispute between an individual and an organisation and quickly escalates from there. One party expresses unhappiness with the other on social media and the other party then responds on social media to defend themselves. During the exchange, personal data is disclosed and is accessible to all and sundry. The approach of the Personal Data Protection Commission ("PDPC") in such cases has been stated in *Re My Digital Lock Pte Ltd*[1] and *Re M Stars Movers & Logistics Specialist Pte Ltd*[2] and that approach has been followed in this case.

2 The Organisation is a sole-proprietorship in the scuba-diving services business. The Complainant is an ex-employee of the Organisation.

3 The key issue is whether by using the personal data, the Organisation has:

(a) breached its obligation under s 13 of the Personal Data Protection Act 2012[3] ("PDPA") to obtain valid consent before disclosing personal data; or
(b) breached its obligation under s 18 of the PDPA to only use and disclose personal data for purposes (i) that a reasonable person

1 [2018] PDP Digest 334.
2 [2018] PDP Digest 259.
3 Act 26 of 2012.

would consider appropriate in the circumstances; and (ii) that the data subject has been informed of.

MATERIAL FACTS

4 The Complainant and the Organisation had a contractual dispute in which the Complainant claimed that the Organisation had failed to pay his wages. The Complainant resigned and took dive equipment which he claims to have paid for.

5 The Organisation, however, refutes these claims and says that it withheld $600 from the Complainant as the Complainant owed the Organisation $850 for participating in and logging dives organised by the Organisation with the aim of the Complainant obtaining the PADI Dive Master Certification. Also, the Organisation alleges that the Complainant did not pay for the dive equipment that he took and instead stole the said equipment together with the Organisation's documents. Accordingly, the Organisation has filed a police report against the Complainant for the alleged theft.

6 The above contractual dispute and allegations of theft are beyond the remit of the PDPC and I do not make any findings in respect of the above. It is the actions of the Organisation and the Complainant subsequent to the submitting of the police report that concern the PDPC. According to the Complainant, the Organisation had sent text messages to some of its customers informing them of allegations against the Complainant.

7 In February 2018, the Complainant wrote a Facebook post detailing his unhappiness with the Organisation and its sole proprietor. The crux of his post was that he felt cheated because the Organisation did not pay his salary and made a police report against him although he did his best as an employee. He also warned other divers from joining the Organisation.

8 The Organisation responded with two Facebook posts of its own, which were posted on the Facebook pages of the sole-proprietor (*ie*, his personal Facebook page) and a public group for scuba divers. The crux of these posts was that the Complainant owed the Organisation money for participating in dives organised by them, that they had given him a large discount to participate in the dives, that they had given the Complainant diving experience that no one else would give him and that the

Complainant stole diving equipment as well as a customer database and the Organisation's delivery documents.

9 The Organisation also disclosed the following personal data in these posts: (a) the Complainant's name, NRIC number, date of birth, passport number and expiry date, mobile phone number, e-mail address and residential address; and (b) the name and residential address of the Complainant's female friend as well as the make of her car (collectively, the "Personal Data Sets"). It is undisputed that the Personal Data Sets were in the Organisation's possession and that the Organisation had obtained them from the Complainant when he was employed by the Organisation.

DID THE ORGANISATION COMPLY WITH SECTIONS 13 AND 18 OF THE PERSONAL DATA PROTECTION ACT?

10 Subject to certain exceptions,[4] in accordance with s 13 read with s 14 of the PDPA, organisations may only collect, use or disclose personal data about an individual with the consent of that individual (the "Consent Obligation"). It is undisputed that the Organisation had not explicitly obtained the Complainant's consent to disclose the Personal Data Sets in the manner above or notified him, as required under s 20 of the PDPA, that his personal data would be disclosed in such manner.

11 In *Re M Stars Movers*, the position I took was as follows:

> 18 The Deputy Commissioner advises caution in disclosing personal data when responding to public comments. An organisation should not be prevented or hampered from responding to comments about it using the same mode of communications that its interlocutor has selected. In some situations, it may be reasonable or even necessary to disclose personal data in order to advance an explanation. An individual who makes false or exaggerated allegations against an organisation in a public forum may not be able to rely on the PDPA to prevent the organisation from using material and relevant personal data of the individual to explain the organisation's position on the allegations through the same public forum.
>
> 19 The following observations may be made in this context about the approach that the Commission adopts. First, the Commission will not engage in weighing allegations and responses on golden scales in order to

4 Pursuant to s 17 of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA") read with the Second, Third and Fourth Schedules of the PDPA.

> establish proportionality. The better approach is to act against disclosures that are clearly disproportionate on an objective standard before the Commission intervenes in what is essentially a private dispute …

12 In the present case, the Organisation's disclosure of personal data is clearly disproportionate on any objective standard. I can conceive of no legitimate reason for the Organisation to disclose the Complainant's NRIC and passport number in order to defend itself against the Complainant's allegations. Neither can I see the relevance of disclosing the name and residential address of the Complainant and the make of the car owned by the Complainant's friend to the dispute over salary and dive equipment.

13 While it is understandable how such excessive disclosure of personal data could have been made when penning social media posts in the heat of the moment, such conduct is nevertheless inexcusable. Let this be a caution against wielding one's pen in anger during the heat of altercation.

14 I thus find that the Organisation's disclosure of the personal data of the Complainant and his friend was done without consent and is in breach of s 13 of the PDPA.

ACTIONS TAKEN BY THE COMMISSION

15 As at 15 March 2018, the Facebook posts had been removed. Upon being contacted by the Personal Data Protection Commission, the Organisation's sole proprietor resolved to improve his awareness of the Organisation's protection obligations under the PDPA.

16 Having considered these factors and the context in which the breach occurred, I have decided to issue a warning to the Organisation for breaching its obligations under s 13 of the PDPA, without further directions or imposing a financial penalty.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re WTS Automotive Services Pte Ltd

[2019] PDP Digest 317

Coram: Tan Kiat How, Commissioner
Case Number: DP-1706-B0834
Decision Citation: [2019] PDP Digest 317; [2018] SGPDPC 26

Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

13 December 2018

BACKGROUND

1 This matter involves WTS Automotive Services Pte Ltd (the "Organisation"), a company which provides vehicle repair and maintenance services at Kaki Bukit and Gul Circle in Singapore. On 9 June 2017, a complaint was lodged by a member of the public ("Complainant") with the Personal Data Protection Commission ("Commission"), alleging that a URL to the Organisation's customer database, which contained the personal data of the Organisation's customers, was publicly accessible over the Internet (the "Incident"). The Commissioner sets out below his findings and grounds of decision based on the investigations carried out in this matter.

MATERIAL FACTS

2 The Complainant had been searching for a company address via Google's search engine, when he chanced upon the URL to the Organisation's Kaki Bukit customer database, which contained the personal data of 2,472 of its Kaki Bukit customers. The personal data that was disclosed included the names, NRIC numbers and FIN, residential addresses, contact numbers, e-mail addresses and car plate registration numbers of the Organisation's Kaki Bukit customers. The Complainant proceeded to lodge a complaint with the Commission on 9 June 2017.

Upon receiving the complaint, the Commission commenced an investigation into this matter.

3 During the course of the investigation, the Organisation represented that it had implemented a Backend Electronic Job Card System ("Backend System") which ran as a web application over the Internet since December 2013. The Backend System was set up for internal use only and was meant to allow the Organisation's staff to, amongst other things, store and access the personal data of the Organisation's customers. The Backend System was developed and maintained by ZNO International (Pte) Limited ("ZNO") from October 2013. Subsequently, QGrids was responsible for the maintenance of the Backend System from March 2016. The Organisation represented that the publicly accessible URL to the Organisation's Kaki Bukit customer database was part of the Backend System.

4 During the course of the investigation, the Commission also found that there were two other databases that were part of the Backend System, which similarly contained personal data and were also publicly accessible, as follows:

(a) the Organisation's Gul Circle customer database, which contained the names, NRIC numbers and FIN, residential addresses, contact numbers, e-mail addresses and car plate registration numbers of 2,223 of the Organisation's Gul Circle customers; and

(b) the Organisation's master car database, which contained 3,764 records with the names of car owners, and the details of their cars, such as a car's make, model, plate number, colour, chassis number, registration number, transmission type and mileage.

5 All three URLs to the Organisation's three databases will collectively be referred to as the "Compromised URLs". The Compromised URLs were all webpages which provided data export functions, *ie*, they allowed data to be exported into Microsoft Excel spreadsheets. By clicking on any of the Compromised URLs, the corresponding Microsoft Excel spreadsheet would be generated and provided to a user. As the Microsoft Excel spreadsheets would subsequently be saved in the backend server, the Microsoft Excel spreadsheets could be discovered and indexed by search engines.

6 Notably, the Organisation admitted during the course of the investigation that the webpages of the Backend System were all secured by authentication mechanisms, save for the Compromised URLs. The

Organisation represented that the authentication mechanisms for the Compromised URLs were "*left out by ZNO unintentionally*" during the development of the Backend System. With no authentication mechanisms to limit access to the Compromised URLs, search engines were able to discover and index these Compromised URLs, rendering the respective databases publicly accessible over the Internet.

7 After the Organisation was notified by the Commission of the unauthorised disclosure of its Kaki Bukit customers database on 15 June 2017, the Organisation represented that it had taken the following steps to prevent the reoccurrence of the unauthorised disclosure of personal data:

(a) added Robots.txt to discourage search engines from crawling webpages of the Organisation's Backend System;
(b) secured all webpages in the Organisation's Backend System with login mechanisms;
(c) removed the Compromised URLs from Google and Bing search engines; and
(d) migrated the Backend System to a local server and configured it to be accessible only within the Organisation's Local Area Network instead of the Internet.

8 At the outset, the information that was disclosed via the Compromised URLs (names, NRIC numbers and FIN, residential addresses, contact numbers, e-mail addresses, car plate registration numbers and details of cars, such as a car's make, model, plate number, colour, chassis number, registration number, transmission type and mileage) constitutes personal data as defined in s 2(1) of the Personal Data Protection Act 2012[1] ("PDPA"), as the Organisation's customers and/or car owners could be identified from such information disclosed or is information that is about these identified customers and/or car owners.

9 The issue for determination is whether the Organisation, ZNO and QGrids had complied with the obligation under s 24 of the PDPA to implement reasonable security arrangements to protect personal data in its possession or under its control.

1 Act 26 of 2012.

10 Section 24 of the PDPA provides:

> 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. [emphasis added]

As a preliminary issue, the meaning of the terms "possession" and "control" under s 24 of the PDPA is considered. Whilst the definition of "possession" is not defined in the PDPA, the distinction between "possession" and "control" had been explained in *Re The Cellar Door Pte Ltd*[2] at [17] as:

> [I]t 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.

11 Notably, in *Re The Cellar Door Pte Ltd*, it was found that even though the organisation was not in direct possession of the personal data that was held in the data intermediary's servers, it was still obliged to implement reasonable security arrangements to protect the personal data as it had control over such data.

12 As to the definition of "control", *Re AIG Asia Pacific Insurance Pte Ltd*[3] at [18] states that:

> While there is no definition of 'control' in the PDPA, the meaning of control in the context of data protection is generally understood to cover *the ability, right or authority to determine (a) the purposes for; and/or (b) the manner in which personal data is processed, collected, used or disclosed.* [emphasis added]

13 Against this backdrop, the issue for determination is whether the Organisation, ZNO and QGrids each had possession or control of the personal data contained in the Compromised URLs, so as to trigger the obligation to implement reasonable security arrangements to prevent its unauthorised disclosure under s 24 of the PDPA.

---

2 [2017] PDP Digest 160.

3 [2019] PDP Digest 189.

Whether ZNO International (Pte) Limited had the obligation to protect personal data under section 24 of the Personal Data Protection Act

14 ZNO was the IT vendor engaged by the Organisation to develop, host and maintain the Backend System. While the Organisation claims that it had asked ZNO to include authentication mechanisms to limit access to the data found in the Compromised URLs, the only evidence that the Organisation relied upon was the statement of its general manager. Even if we take the Organisation's case at its highest and it is found that ZNO was indeed asked to implement authentication mechanisms, ZNO would not be in breach of the PDPA given that it had delivered the Backend System (save for one module which was not relevant to the Incident) in 2013. After the relevant PDPA provisions came into force on 2 July 2014, the onus is on the Organisation to review its existing systems and to put in place enhancements to ensure that the standards of protection under the PDPA are met. In this regard, the Commissioner finds that ZNO did not have the obligation under s 24 of the PDPA.

Whether QGrids had the obligation to protect personal data under section 24 of the Personal Data Protection Act

15 As of March 2016, QGrids had been engaged by the Organisation for the purposes of application and data migration from ZNO's web hosting services to Vodien Internet Solutions Pte Ltd ("Vodien"), a third-party Singapore-based web hosting company which provides, amongst other services, domain registration and web hosting services, and subsequently, to take over the maintenance of the Backend System from ZNO. QGrids had possession of the personal data, which is the subject of this decision, in migrating the Backend Server to Vodien and would have had to ensure that such personal data was protected. However, the data breach that occurred in this case was not a result of the migration of the Backend Server or QGrids's role with respect to this. In this regard, the Commissioner finds that QGrids does not have the obligation under s 24 of the PDPA to implement reasonable security arrangements to protect the personal data contained in the Compromised URLs.

Whether the Organisation had the obligation to protect personal data under section 24 of the Personal Data Protection Act

16 With regard to the development of the Backend System, the Organisation represented that it had "[specified] to ZNO that the website and system should be protected with login mechanism and role-based authorisation feature; however, these requirements were given verbally during requirement analysis and were not recorded in any document". Also, while the Organisation represented that it had tested the Backend System before it was delivered to the Organisation by ZNO, the user acceptance test was not documented by either the Organisation or ZNO.

17 The Commissioner takes this opportunity to reiterate the importance of clarifying the obligations of an organisation and a service provider and thereafter documenting these in writing and prior to the provision of services, as set out in *Re Smiling Orchid (S) Pte Ltd*[4] at [51]:

> 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.

18 Presently, there is an absence of objective evidence showing that the Organisation had given specific requirements that login mechanism and role-based authorisation were required. Equally, there is no evidence that this requirement was communicated, documented or – crucially – included within the scope of user acceptance tests. Post 2 July 2014 when the PDPA came into full force, the Organisation should have reviewed its systems to ensure that the standards of protection expected under the PDPA are met. The Commission also recognises that "personal data of individuals may be exposed if the website or database in which it is stored contains vulnerabilities. There needs to be a regular review to ensure that the website collecting personal data and the electronic database storing the personal data has reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks".[5] The Commission considers that it is good practice for an organisation to "[c]onduct regular ICT security audits, scans and tests to detect

4 [2017] PDP Digest 133.

5 Personal Data Protection Commission, *Guide to Data Protection Impact Assessments* (1 November 2017) at para 8.3.

vulnerabilities".[6] Against the above backdrop, the Organisation retained full responsibility for implementing reasonable security arrangements to protect the personal data contained in the Compromised URLs. The Commission found that the Organisation did not take any steps towards protecting the personal data in its possession or under its control to prevent any unauthorised disclosure of the personal data contained in the Compromised URLs. Additionally, it should have conducted regular IT security checks to ensure that the Backend System did "not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the Internet".[7]

19 Although access to the Backend System was only intended for staff of the Organisation, considering how the Backend System was accessible from the Internet, it would have been important for the Organisation to conduct IT security checks to detect vulnerabilities in the Backend System. The Commission takes the view that "[t]esting the website for security vulnerabilities is an important aspect of ensuring the security of the website. Penetration testing or vulnerability assessments should be conducted prior to making the website accessible to the public, as well as on a periodical basis (e.g. annually)".[8] In this regard, the Organisation represented that "there [was no] penetration testing performed prior to [the Commission notifying the Organisation about the unauthorised disclosure of personal data on 15 June 2018]".

20 Given the absence of any security arrangements to protect personal data against unauthorised disclosure, the Commissioner finds that the Organisation has contravened s 24 of the PDPA.

REPRESENTATIONS

21 The Organisation made representations following the issuance of a preliminary Grounds of Decision. The Commissioner has considered the representations made and is of the view that the representations made do

6 Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017) at para 6.1.

7 Personal Data Protection Commission, *Guide on Building Websites for SMEs* (revised on 20 January 2017) at para 4.2.1.

8 Personal Data Protection Commission, *Guide on Building Websites for SMEs* (revised on 20 January 2017) at para 5.6.1.

not justify any change in his decision or the directions made. The Commissioner sets out below the points raised in the representations together and the reasons for rejecting the representations.

22 The Organisation in its representations stated that it had implemented a role-based authorisation feature and a login mechanism. These facts have already been taken into consideration. The Organisation's claims that it had instructed its vendor to protect the system with a login mechanism and a role-based authorisation feature are considered in [18] above. Even on the assumption that instructions for a role-based authorisation feature and a login mechanism were properly given, the authentication mechanisms were not implemented with respect to the Compromised URLs and any alleged instructions were not documented. As stated in [17], such instructions should be documented in writing to clarify the obligations of an organisation and a service provider.

23 The Organisation also stated in its representations that it had expected its vendor ZNO to conduct all the necessary audits as it was still developing the backend system even after the relevant data protection provisions under the PDPA came into force in July 2014 and that the disclosure resulted from a programming flaw. This has already been considered at [14] above. Further, organisations should take note that while they may delegate work to vendors to comply with the PDPA, the organisations' responsibility for complying with statutory obligations under the PDPA may not be delegated. In this case, the Organisation simply did not put in place any security arrangements to ensure that it complied with its obligations under s 24 of the PDPA.

24 The final point made by the Organisation in its representations is that it had no technical expertise to identify technical flaws and had no reason to suspect that the Compromised URLs would be published on the Internet. In the present case, the gravamen lies in the lack of awareness and initiative on the part of the Organisation, as owner of the system, to take its obligations and responsibilities under the PDPA seriously. It is unrealistic to expect all organisations to have the requisite level of technical expertise to manage increasingly complex IT systems. But a responsible organisation would have made genuine attempts to engage competent service providers and give proper instructions. In this case, it is the paucity of evidence of such instructions, purportedly made by the Organisation, that stands out. Likewise, there was no evidence that it had conducted adequate testing of

the system. Pertinently, while these lapses may have been more excusable before 1 July 2014, there is no excuse for the Organisation not to have initiated (and properly documented) a review of the system for compliance with the PDPA. The responsibilities of ownership do not require technical expertise.

DIRECTIONS

25 Having found that the Organisation is in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

26 In assessing the breach and determining the directions to be imposed on the Organisation, the Commissioner took into account the following mitigating factors:

(a) the Organisation was generally co-operative, forthcoming and prompt in providing responses to the Commission during the investigation; and
(b) the Organisation took immediate remedial actions to rectify and prevent the recurrence of the data breach.

27 The Commissioner also took into account the aggravating factor that the Organisation showed a lack of accountability with respect to the Backend System and its obligation to protect the personal data that was stored on it. Not only did the Organisation fail to document the instructions given to ZNO to implement login mechanism and role-based authorisation features for the Backend System, the Organisation had also failed to document the user acceptance test. While the system was developed and delivered before the PDPA came into full force, the Organisation, knowing full well that its practices left a lot to be desired from a security standpoint, ought to have audited its systems before 2 July 2014 to ensure that its practices are PDPA compliant. The failure to do so reflected the Organisation's lack of accountability in ensuring that it had made reasonable security arrangements to protect the personal data on the Backend System, as well as to prevent any unauthorised disclosure or similar risks to such data.

28 In consideration of the relevant facts and circumstances of the present case, the Commissioner hereby directs the Organisation to pay a financial

penalty of S$20,000 within 30 days from the date of this direction, failing which interest, at the rate specified in the Rules of Court[9] in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

9 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re SLF Green Maid Agency

[2019] PDP Digest 327

Coram: Yeong Zee Kin, Deputy Commissioner
Case Number: DP-1806-B2265
Decision Citation: [2019] PDP Digest 327; [2018] SGPDPC 27

Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

13 December 2018

BACKGROUND

1 This case arose out of the common practice of reusing scrap or discarded paper where the reverse side of the paper can still be used. This is highly commendable and environmentally-friendly, but organisations must take care to ensure that there is no personal data on the scrap or discarded paper set aside for such reuse. An employee of SLF Green Maid Agency (the "Organisation") wrote information for the Complainant on a piece of paper which contained personal data of other individuals on the reverse side and gave the paper to the Complainant. This happened on two separate occasions. The key issue is whether this disclosure of personal data by the Organisation amounts to a breach of s 24 of the Personal Data Protection Act 2012[1] ("PDPA").

MATERIAL FACTS

2 On 8 April 2018, the Complainant visited the Organisation's office to enquire about engaging a foreign domestic worker. An employee of the Organisation assisted her and over the course of these enquiries, the employee handed the Complainant some paper on which he wrote

1 Act 26 of 2012.

information related to her query. The Complainant discovered that the reverse side of the paper contained personal data of other individuals. The Complainant informed the employee that the paper that was used should not have been given to the Complainant.

3 On 24 April 2018, the Complainant returned to the Organisation's office and was served by the same employee. Again, over the course of the queries, she was provided information handwritten on used paper. Similarly, the reverse side of the paper contained personal data of other individuals.

4 Over the two occasions, the following personal data was disclosed to the Complainant:

(a) On the first occasion, the used side of the paper contained a photocopy of the front and back of an individual's NRIC.

(b) On the second occasion, the used side of the paper was a letter detailing a family's personal circumstances, explaining why a foreign domestic worker was required by them. The letter also contained four individuals' names and two of their FIN numbers. In an accompanying portion of a contract, the same four individuals' passport numbers and passport expiry dates were found; and

(c) the same portion of a contract contained five other individuals' names and NRIC numbers, with some accompanying signatures.

DID THE ORGANISATION BREACH SECTION 24 OF THE PERSONAL DATA PROTECTION ACT?

5 Section 24 of the PDPA stipulates 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. It is undisputed that the personal data listed in [4] was disclosed without authorisation. The totality of the circumstances led me to conclude that the unauthorised disclosure stemmed from the Organisation's lack of reasonable security arrangements to prevent such disclosure. I set out the factors leading to this conclusion below.

6 Organisations that reuse scrap paper should put in place reasonable security measures to prevent scrap paper containing personal data from being reused or given to other clients. The security arrangements will have to involve at least two aspects:

(a) implementing a system of processes backed up by policies; and
(b) training staff to be aware of the risks and to be alert to spot them.

7 In this case, investigations did not turn up any process or system within the organisation for segregating scrap paper containing personal data from the pile(s) of scrap paper that can be reused by staff.

8 Neither were there any policies. In fact, the Organisation admitted that it did not have a detailed policy with respect to personal data protection nor did it provide staff with any formalised training on personal data. Instead, the Organisation relied on the management's verbal directions to screen through all discarded paper and to destroy any paper that contained personal data; and that only paper which did not contain personal data was to be reused. The Organisation intimated, in written responses during investigations, that the following instructions were given to employees:

> Physical Office Manning- Office should be manned continuously by staff during operating hour. In occasion that staff is alone in office and the need to leave the office, say go to the toilet, office should be locked. Do not leave office open but unattended.
>
> Management of Client's data- Clients (Employer/customer and FDW) data should not be used or discussed loosely. Not even between staff and staff. Management insists that no loose talk on sensitive data like how rich is an employer and personal income, where employer stays, etc … Only on a need to know and authorized to know basis.
>
> Clients/FDW's document. Individual client/FDW's document are filed and serialized. Files are safe keep in cabinet within the office space which is locked after office hour.
>
> Access to Personal Computer. Instruction to all staff is that 'outsider' person who is not authorized is not allowed to 'touch' our personal computer. Ever happened before that a staff let a customer use her personal computer to check certain thing from website was reprimanded.

9 To my mind, these instructions were insufficient and failed to establish the practices around the Organisation's policy of using discarded paper that contained personal data.

10 The Organisation intimated that they prominently pasted a set of guidelines on handling personal data and provided a copy of a document entitled "Guidelines to Personal Data Protection" ("Organisation's "Guidelines"). The relevant part of the Organisation's "Guidelines" stated:

> *Proper Housekeeping Other than the document that Staff is working on at any point in time, no other unnecessary document, especially document with personal data should be lying around on the working table or other places.*
>
> …
>
> *Management of waste paper with personal information on it. Waste paper with personal data on them are not to be disposed of in public rubbish bin direct, unless data is permanently masked off by using permanent marker and is torn into small pieces.*
>
> [emphasis in original]

11 There are a couple of issues with the Organisation's Guidelines. First, they do not address the reuse of discarded paper containing personal data directly. They deal with safekeeping and disposal of waste paper containing personal data. Second, investigations did not uncover any evidence to substantiate that the Organisation's Guidelines were provided to its employees.

12 Turning now to the importance of staff training as a security arrangement. It has been said before in *Re National University of Singapore*[2] and it bears repeating that training is important to inculcate the right employee culture and establish the right level of sensitivity to personal data amongst staff. The organisation admitted that no training had been provided. The closest form of training in this matter was a verbal exhortation by management to screen scrap paper and to discard (and not to reuse) scrap paper that contained personal data. Clearly, this was insufficient to establish the right level of employee sensitivity to client personal data. These verbal instructions did not appear to have been effective on the employee who served the Complainant as he made the same mistake to the same client twice: he handed over to the Complainant scrap

2 [2018] PDP Digest 155.

paper containing personal data of other individuals on two separate occasions and had failed to retrieve them even after the employee was informed by the Complainant that he should not reuse paper with personal data.

13 For a company like the Organisation that handles personal data of foreign domestic workers and clients on a daily basis (*eg*, passport and income information), it is necessary for it to put in place a better system of staff training and awareness given the sensitive nature of personal data that it handles, as well as the volume. Merely disseminating guidelines and verbal instructions is insufficient. As noted in *Re Aviva Ltd*,[3] whilst there is no specific distinction in the PDPA based on the sensitivity of the data, organisations are to ensure that there are appropriate levels of security for data of varying levels of sensitivity. NRIC and passport numbers and financial information would generally be considered more sensitive.[4] Structured and periodic training could have been implemented to protect personal data.

14 I therefore find that the Organisation was in breach of its obligation to protect personal data under s 24 of the PDPA as it did not implement reasonable security arrangements to protect the personal data found in the discarded papers. Since the incident, the Organisation has reminded its staff to comply with internal guidelines on personal data protection and the procedures for destroying documents containing personal data. It has also highlighted to the staff internal penalties for any failure to comply.

DEPUTY COMMISSIONER'S DIRECTIONS

15 Given my findings that the Organisation is in breach of s 24 of the PDPA, I am 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 S$1m.

16 Taking into account the limited scope of the unauthorised disclosure, I do not think that a financial penalty is warranted and instead make the following directions:

---

3 [2018] PDP Digest 245 at [17]–[18].

4 *Re Aviva Ltd* [2018] PDP Digest 245 at [17].

(a) the Organisation is to conduct a review of its procedures to prevent the use of discarded or unwanted documents containing personal data within 30 days from the date of this decision;

(b) the Organisation is to develop a training programme to ensure that all of its staff are aware of and will comply with the requirements of the PDPA when handling personal data within 60 days from the date of this decision;

(c) the Organisation is to require all staff who have not attended data protection training to attend such data protection training in accordance with the training programme set out at (b) above within 30 days of the development of the training programme; and

(d) the Organisation is to inform the Commission of the completion of each of the above within seven days of implementation.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Institute of Singapore Chartered Accountants

[2019] PDP Digest 333

Coram: Tan Kiat How, Commissioner
Case Number: DP-1711-B1367
Decision Citation: [2019] PDP Digest 333; [2018] SGPDPC 28

Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

13 December 2018

BACKGROUND

1 Technology has transformed the way we communicate. Today, we live in a world of tweets and texts, e-mail and instant messaging. This case shows that when sending documents containing a significant volume of personal data by e-mail, it is important for organisations to have in place reasonable security arrangements to protect these documents from unauthorised access by unintended recipients.

2 On 27 November 2017, the Personal Data Protection Commission (the "Commission") received notification from the Institute of Singapore Chartered Accountants ("ISCA") that one of its employees inadvertently sent an e-mail attaching a Microsoft Excel document containing the personal data of 1,906 individuals (the "Excel File") to an unintended recipient (the "Incident").

3 Following an investigation into the matter, the Commissioner found ISCA in breach of s 24 of Personal Data Protection Act 2012[1] ("PDPA").

1 Act 26 of 2012.

MATERIAL FACTS

4 Established in 1963, ISCA is the national professional body for accountants in Singapore with about 32,000 members. ISCA is the administrator of the Singapore Chartered Accountant Qualification and the designated body to confer the "Chartered Accountant of Singapore" designation.

5 On or about 23 November 2017, as part of business operations, two ISCA employees (the "First Employee" and the "Second Employee", collectively the "Employees") were unable to open the Excel File (stored on ISCA's internal shared drive) as it appeared to be corrupted. The Employees sought the assistance of ISCA's IT department. Arising from this, ISCA's IT Support Specialist sent an e-mail to the System/Network Engineer from the ICT department to recover the Excel File from the backup server, and to send the recovered Excel File to the Employees.

6 On 24 November 2017, the System/Network Engineer created an e-mail to send the recovered Excel File as an attachment to the Employees (the "Subject E-mail"). As the earlier e-mail from the IT Support Specialist did not include the Employees in the addressee list, the System/Network Engineer had to specifically insert the Employees in the recipient section of the Subject E-mail. Due to the auto-complete feature in Microsoft Outlook's e-mail software, the System/Network Engineer inadvertently selected an accounts manager (the "Unintended Recipient")[2] in a listed telecommunications service provider ("Telco") instead of the First Employee as they both had the same first name. The Subject E-mail containing the Excel File was therefore sent to the IT Support Specialist, the Second Employee and the Unintended Recipient. The Excel File was not encrypted with a password.

7 The Excel File listed 1,906 candidates in the ISCA Professional Examination programme. The personal data[3] of the candidates which were disclosed include the following:

---

2 The Unintended Recipient was the designated accounts manager to communicate with the Institute of Singapore Chartered Accountants ("ISCA") on services provided by the Telco to ISCA.

3 Each of the 1,906 candidates did not have the same types of data disclosed in the Excel File. Some candidates had more data in the Excel File than others.

(a) NRIC numbers;
(b) passport numbers;
(c) name;
(d) date of birth;
(e) postal address;
(f) e-mail address;
(g) mobile phone numbers;
(h) employment history records;
(i) qualification records;
(j) exam results; and
(k) appeal status of their candidature.

(collectively, the "Subject Data")

8 The Second Employee discovered the mistake within ten minutes of the Subject E-mail being sent, and reported it to the Manager, Info-communications and Technology Management, who was also one of ISCA's data protection officers (the "Manager ICT").

9 ISCA took the following remedial action:

(a) On 24 November 2017 at around 3.24pm, the System/Network Engineer e-mailed the Unintended Recipient to inform her to disregard the Subject E-mail. At around 3.44pm, the Unintended Recipient replied the System/Network Engineer to inform ISCA that she had deleted the Subject E-mail without opening the Excel File.
(b) On 25 November 2017, the Manager ICT sent a further e-mail to the Unintended Recipient to require that all copies of the Subject E-mail and Excel File are permanently deleted. Through e-mails dated 27 and 28 November 2017, the Unintended Recipient confirmed that the Subject E-mail and Excel File have been permanently deleted.
(c) The Unintended Recipient signed a declaration confirming that:
    (i) the Subject E-mail and Excel file were promptly deleted upon the Unintended Recipient being notified by ISCA of the Subject E-mail being sent by mistake;
    (ii) the Excel File was not opened by the Unintended Recipient nor anyone else; and

(iii) the Unintended Recipient's employer does not possess the Subject E-mail and Excel File and no copies remain in its mail servers, backups or systems.

(d) On 29 November 2017, ISCA notified all 1,906 candidates of the Incident by e-mail and/or SMS.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

10 It is not disputed that the Subject Data is "personal data" as defined in s 2(1) of the PDPA. There is also no dispute that the PDPA applies to ISCA as it falls within the PDPA's definition of "organisation".

11 The issue to be determined by the Commissioner in this case is whether ISCA had complied with its obligations under s 24 of the PDPA.

Whether Institute of Singapore Chartered Accountants complied with its obligations under section 24 of the Personal Data Protection Act

12 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.

13 It is not disputed that ISCA had possession and/or control of the Subject Data in the Excel file stored on ISCA's internal shared drive and backup server.

Institute of Singapore Chartered Accountants' security arrangements to protect electronic documents containing personal data

14 As part of ISCA's business operations, its employees are required to access a significant number of its members' personal data contained in electronic files (*eg*, the Excel File contained 1,906 individuals' Subject Data). The Subject Data in ISCA's possession and/or control included personal data which has a higher expectation of confidentiality (*eg*, employment history records, qualification records, exam results and appeal status) and could be potentially embarrassing if disclosed to unauthorised recipients.

15 In this regard, ISCA has a general policy that applies to the whole organisation with respect to the protection of personal data of its members. This "Information Sensitivity Policy" is intended to guide employees on protecting information at varying sensitivity levels, including during electronic distribution. According to ISCA, the Subject Data in the Excel File would fall under the "More Sensitive" category. For electronic distribution of documents in this category, there are "no restrictions to approved recipients within ISCA, but should be encrypted or sent via a private link to approved recipients outside of ISCA premises".

16 ISCA also has targeted policies and standard operation procedures ("SOPs") for specific departments and/or operational activities that deal with personal data. The policies/SOPs that require electronic documents containing personal data to be protected are:

(a) "Data Management for CPE Programmes Policies and Procedures" applies to employees dealing with continuing professional education. It requires encryption for Excel reports generated that contains personal data.

(b) "Data Management" applies to the Member Services and Marketing department of ISCA. It requires internal reports generated by the department that contain personal data to be "encrypted with password".

(c) The SOP entitled "Student Data Management" attached two e-mails in relation to the protecting files that contain personal data which stated:

(i) "Please ensure that your files are password-protected especially if they contain personal data such as name, NRIC number, address, phone number and email address"; and

(ii) "For electronic transmission (i.e. email, thumbdrives etc) of personal data, please ensure the files are encrypted".

17 However, none of ISCA's security arrangements at [15] and [16] required password-based encryption for the Excel File in the circumstances leading up to the Incident.

(a) ISCA's Information Sensitivity Policy did not apply because the System/Network Engineer intended to send the Excel File by e-mail to authorised recipients within ISCA only.

(b) ISCA conceded that none of the policies/SOPs at [16] applied to the System/Network Engineer who was in ISCA's ICT department.

18 The Commissioner found that ISCA failed to put in place reasonable security arrangements to protect the Subject Data in the Excel File during e-mail transmission for the following reasons:

(a) The volume (1,906 members) and type (data with a higher expectation of confidentiality) of Subject Data in the Excel File warranted direct protection. In this regard, ISCA should have had a policy/SOP that applied to all employees requiring password-based encryption for the Excel File in respect of both external and internal e-mails. This would be a reasonable security arrangement to protect the Subject Data against unauthorised access in the event the Subject E-mail was sent to any unintended recipient.

(i) ISCA's Information Sensitivity Policy at [15] was not a sufficient security arrangement as it only required password-based encryption for external e-mails.

(ii) ISCA's "Student Data Management" SOP at [16(c)] recognised that the Subject Data in the Excel File required direct protection. Under this SOP, the Employees who had requested the Excel File would have had to ensure that the Excel File is encrypted with a password for electronic transmission. However, as discussed at [17(b)], this SOP did not apply to the System/Network Engineer. At the material time, ISCA did not have a specific policy/SOP for the ICT department in respect of its operational activities that deal with personal data.

(iii) According to ISCA, the System/Network Engineer did not open the Excel File when recovering it from ISCA's backup server. He was therefore not aware that the Excel File did not have password-based encryption. This excuse is not credible for the reason that when the Employees requested for the restoration of an Excel file from the backup server, one would have expected that the least that would have been done was for the System/Network Engineer to open the file to be sure that it had been properly restored and thus usable by the Employees. It is

more likely that the System/Network Engineer had opened the file, but it had not occurred to him that it was a spreadsheet containing voluminous personal data. In any event, the lack of policy/SOP for the ICT department and the gap in the extant Information Sensitivity Policy meant that the System/Network Engineer would not have been required to password-protect the restored Excel file.

(b) ISCA conducted PDPA training for its employees. In this regard, data protection training only has an impact on the proper implementation of an organisation's data protection policies and practices. It does not replace the requirement for an organisation to have the necessary data protection policies in respect of its operational/business activities that deal with personal data. In the present case, ISCA did not have any policy/SOP that if properly implemented, would have been a reasonable security arrangement to protect the Excel File during internal e-mail transmission.

19 For the reasons above, the Commissioner finds ISCA in breach of s 24 of the PDPA.

REPRESENTATIONS BY INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

20 ISCA made representations following the issuance of a preliminary decision to ISCA. The representations did not go to the merits of the matter but were mainly related to the timelines for ISCA to comply with the Commissioner's directions. The Commissioner has considered the representations made and has made adjustments to the timelines in the final set of directions below.

THE COMMISSIONER'S DIRECTIONS

21 Given the Commissioner's findings that ISCA is in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to issue ISCA such directions as it deems fit to ensure compliance with the PDPA. This may include directing ISCA to pay a financial penalty of such amount not exceeding S$1m.

22 In assessing the breach and determining the directions, if any, to be imposed on ISCA in this case, the Commissioner took into account the following mitigating factors:

(a) ISCA notified the Commission of the Incident and was fully co-operative in the investigations;
(b) the unauthorised disclosure was limited to a single Unintended Recipient for a short period of ten minutes;
(c) ISCA took prompt action to mitigate the impact of the Incident by (i) requesting the Unintended Recipient to permanently delete the Subject E-mail containing the Excel File; and (ii) notifying all affected individuals of the Incident; and
(d) there was no evidence to suggest any actual loss or damage resulting from the unauthorised disclosure.

23 Having considered all the relevant factors of this case, the Commissioner hereby directs ISCA to do the following:

(a) within 90 days from the date of the Commissioner's directions, review its policies and security arrangements in respect of electronic transmission of documents containing personal data; and
(b) pay a financial penalty of S$6,000.00 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[4] in respect of judgment debts shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

4 Cap 322, R5, 2014 Rev Ed.

Grounds of Decision

Re Funding Societies Pte Ltd

[2019] PDP Digest 341

Coram: Tan Kiat How, Commissioner
Case Number: DP-1708-B1035
Decision Citation: [2019] PDP Digest 341; [2018] SGPDPC 29

Personal data *– Disclosure of financial information – Stronger controls needed to protect sensitive personal data*
Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*

13 December 2018

BACKGROUND

1 On 14 August 2017, the Personal Data Protection Commission (the "Commission") received an e-mail notification from the Organisation. The Organisation is the operator of an online financing platform that connects borrowers and investors (the "Website"). Individuals who used the Website would have to register for an account, either as an "Investor" or a "Borrower" (collectively, "Members"). Each Member was given a unique identifier, which was generated sequentially (the "Member ID").

2 In its e-mail notification, the Organisation informed the Commission that one of its Members, [Redacted] (replaced with "Mr J"), had e-mailed them on 25 July 2017 to inform that he had found a vulnerability with the Website. To illustrate this, Mr J showed the Organisation the personal details of two other Members that he had extracted from the Website (the "data breach"). The Organisation took immediate action to rectify the vulnerability and was able to do so by 26 July 2017.

3 After receipt of the e-mail notification from the Organisation, the Commission proceeded to investigate into an alleged breach of the Personal Data Protection Act 2012[1] ("PDPA").

MATERIAL FACTS

The Website's vulnerability

4 On 19 June 2017, the Organisation rolled out new system components for the Website. This update gave rise to a vulnerability in the Website's security system, the details of which are summarised below.

5 When a Member successfully logged into the Website using his username and password, his browser received an *authentication* token from the Website's server.[2] This token contained the user's Member ID and granted the user access to the Website. Simultaneously, his browser also received an *authorisation* token, containing the same Member ID. The authorisation token controlled the functions and type of data that the particular user could access. Operating together, the two valid tokens (*ie*, authentication and authorisation tokens, which shared the same Member ID) granted the logged-in user access to the Website's functions and data from his own Member account.

6 However, the Organisation's in-house Website developers did not programme the Website to require both tokens to contain the same Member ID. When a logged-in user carried out a browsing activity on the Website, the security system only verified that the user's authentication token was valid, and thereafter granted data access based on the Member ID in the authorisation token, without ensuring that the Member IDs in both tokens were identical.

7 As a result, a Member who had successfully logged into the Website (under an authentication token which carried his Member ID) could

1 Act 26 of 2012.

2 A token is part of the request command from the browser to the Website. Token-based authentication works by ensuring that each request to a server is accompanied by a signed token which the server verifies for authenticity and only then responds to the request.

browse another Member's data by changing the Member ID in the authorisation token. The Organisation suspects that this is how Mr J had gained unauthorised access.

8 The investigations revealed that the Organisation became aware of this vulnerability on 7 July 2017, 18 days before the data breach occurred. The vulnerability was detected by a member of the Organisation's engineering team. Upon discovery, the Organisation initially planned to roll out a quick-fix within a week, and thereafter to have a complete fix within a month.

9 According to the Organisation, a quick-fix was rolled out on 11 July 2017, but had to be retracted on the same day as it caused the Website's mobile applications to crash. The Organisation then worked on finding a fix that would close out the vulnerability without causing the Website's mobile applications to crash.

10 On 20 July 2017, the Organisation rolled out a partial-fix for about 25% of its "endpoints".[3] It did not roll out the entire fix as it wanted to "minimise the chances of inducing a negative effect" on its system. Although there was no evidence that this partial-fix had solved the vulnerability, the Organisation claimed that if Mr J had attempted access through one of the fixed endpoints, he would have been denied access to the data.

11 Before the Organisation could roll out a complete fix for the vulnerability, Mr J informed it of the data breach on 25 July 2017. The Organisation escalated the matter as top priority and rolled out the complete fix within 24 hours of Mr J's report.

12 In total, the vulnerability lasted for about 37 days.

---

3 The Organisation explained that the "endpoint" referred to a function defined on the gateway which had a HTTP URL. The Personal Data Protection Commission understands the "endpoint" in this case to refer to the server which controlled access to its data.

The affected personal data

13 Mr J had accessed and extracted the personal data of two Members. In particular, the personal data that had been extracted included the Members' Customer ID, name, NRIC number, and residential address.

14 While there was no further evidence of unauthorised access, the investigations revealed that the personal data of all the Organisation's existing Members was also at risk of disclosure. At the time of the data breach, the personal data collected and held by the Organisation numbered in the thousands. The personal data that was at risk of disclosure included a Member's Customer ID, NRIC number, account username, first and last name, telephone number, marital status, spouse's name, residential address, bank account details (for investors), subscription agreement (for investors), crowdfunding settings (for investors), suitability assessment settings (for investors), wallet account balance (for investors), and company details (for borrowers).

15 Notably, an unauthorised user would have been able to pretend to be another user by using the other user's Member ID as the authorisation token to perform certain functions in respect of the other user's account. In particular, this included:

(a) using the Investor's account to contact prospective Borrowers;
(b) updating a Member's personal details (subject to actual verification of the details);
(c) providing feedback to the Organisation on behalf of the Member;
(d) changing the Member's e-mail address which was used to subscribe to the Organisation's newsletter; and
(e) altering the auto-investment settings of an Investor's account.

16 With regard to [15(e)], it was revealed that an unauthorised user would have been able to delete the Member's auto-investment settings or alter the parameters for the Member's auto-investment settings. Such an alteration of the auto-investment parameters may have caused the Member to make an investment which he had not initially intended or to fail to make an investment which he may have wanted.

17 There was no evidence that Mr J, or any other person, had performed any of the unauthorised functions in [15].

The Organisation's remedial measures

18 Following the incident, the Organisation immediately requested Mr J to delete the data which he had accessed as a result of the vulnerability. Although the Organisation had requested written confirmation for this, it was only able to obtain verbal confirmation from Mr J that the data had been deleted.

19 The Organisation also took the following remedial actions to resolve the Website's vulnerability:

(a) introducing a more robust logging system to log all unauthorised access to user account data;
(b) forming an internal quality assurance team ("QA team");
(c) implementing documentation requirements which required the QA team to create and maintain details of test cases and test results;
(d) applying secure connection technologies or protocols, such as Transport Layer Security ("TLS") protocol, to all websites and web applications handling personal data;
(e) storing documents containing personal data on Amazon Web Service's Simple Storage Service ("S3"), which allows the storage of data in private buckets that require credential keys which are provided only when requests are authenticated; and
(f) developing and implementing policies and procedures to manage future rollouts of new system components.

FINDINGS AND BASIS FOR DETERMINATION

20 The key issue to be determined is whether the Organisation had complied with its data protection obligations under s 24 of the PDPA.

21 Section 24 of the PDPA requires an organisation to protect the 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 (the "Protection Obligation").

22 As to the standard of reasonable security arrangements, the Commissioner has clarified in *Re Aviva Ltd*[4] that organisations must protect personal information by implementing security safeguards appropriate to the sensitivity of the information and that "more sensitive information should be safeguarded by a higher level of protection".[5]

23 In the present case, the Organisation possessed a wide range of personal data of its Members, including financial information such as bank account details and wallet account balance. The Commissioner considers the financial information of an individual to be "sensitive personal data".[6] It is also noteworthy that such sensitive personal data was readily accessible on the Website via a logged-in account.

24 Having considered the material facts, the Commissioner found that the Organisation did not have reasonable security arrangements in place to prevent the unauthorised access, use and disclosure of personal data in its possession.

25 First, the Organisation did not have adequate security arrangements on its Website to ensure that Members could only access their own information and perform functions on their own accounts. The decoupling of authentication and authorisation into two separate tokens was a deliberate design decision on the Organisation's part so as to "enable stateless API development". However, the Website should have been equipped with a security measure to ensure that the two tokens carried the same Member ID before granting access to data.

26 In the Commissioner's view, implementing such a security measure was a necessary step that the Organisation should have taken after decoupling the tokens. The lack of such security measures was a fundamental mistake on the Organisation's part and left a glaring vulnerability in the Website. Indeed, this vulnerability was so obvious that the Organisation's own engineer had discovered it in the course of his routine work.

27 Second, the Organisation did not adequately test the security of its Website. The Organisation claimed that it had conducted testing prior to

---

4 [2018] PDP Digest 245.

5 *Re Aviva Ltd* [2018] PDP Digest 245 at [19].

6 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [15].

the rollout of the new Website components but was unable to provide documentation of such testing. In any case, the Organisation explained that the tests focused on functionality and load testing of the Website, but not on the security and protection mechanisms. In this regard, it was clear to the Commissioner that the Organisation had failed to conduct the necessary security tests on its Website. Consequently, the Organisation failed to identify the vulnerability during its testing stage.

28 Third, the vulnerability in the Website could be exploited with relative ease. A Member who had some understanding of web technology would have been able to change the Member ID on the authorisation token, thereby granting him access to another Member's profile. While making such a change was not as simple as manipulating the URL, the Commissioner noted that the tools necessary to make such changes were not sophisticated and were readily available online. Crucially, the fact that Member IDs were generated in a sequential order made it even easier for Members to guess other Members' Member IDs.

29 Fourth, the Organisation failed to appreciate the degree of risk that the vulnerability posed to the personal data in its possession. This was evident in its treatment of the vulnerability after its engineer discovered the breach. It had resolved to fix the vulnerability on 7 July 2018 but did not actually prioritise this until the breach occurred on 25 July 2018. The Organisation's explanation that it had only rolled out 25% of the partial fixes to minimise the impact on its system revealed that it was uncertain about the effectiveness and compatibility of the partial fix. It also reflected that it had not taken the vulnerability seriously, and that it was in no rush to fix the vulnerability so long as its business remained operational.

30 As such, the Commissioner finds that the Organisation had failed to make reasonable security arrangements to protect the personal data in its possession and within its control. The Organisation is, therefore, in breach of s 24 of the PDPA.

Representations by the Organisation

31 The Organisation made representations following the issuance of a preliminary decision to the Organisation. The representations did not substantively address the Commissioner's decision to find the Organisation in breach of its obligations under the PDPA but were in the nature of a

request to consider mitigating circumstances. The Commissioner has considered the representations and has decided to maintain the directions in the preliminary decision.

32 The representations made by the Organisation are summarised below:

(a) The Organisation is a relatively young enterprise that has been in operation for less than four years and while it takes "all reasonable efforts to ensure that any security issues and deficiencies are identified, handled and remedied on a proactive basis", there are some issues or deficiencies that it reactively dealt with. In the present case, once the incident was known, the Organisation notified PDPC of its breach voluntarily and expanded reasonable efforts to remediate the incident promptly.

(b) The Organisation continued to assess the data breach incident after its remediation efforts to develop long-term procedures to prevent similar occurrences in the future.

(c) The Organisation had in place a framework of security arrangements, such as a risk management framework, an information security policy and training and audits of its policies and procedures.

(d) Only the data of two individuals was actually disclosed in the incident and no actual loss or damage was suffered; the actual compromised data did not include any financial information. Furthermore, the Organisation received verbal confirmation from the individual who discovered the flaw in the system that he had deleted the personal data of the two individuals that he extracted.

33 The Commissioner did not consider being a young organisation to be a mitigating factor. Neither should the fact that the Organisation continuously assessed its compliance with the obligations set out in the PDPA and that it had the necessary frameworks in place mitigatory as these were the standard of conduct expected for compliance. These are not activities or measures which go beyond the standard of protection required by the PDPA and as such are not mitigating factors.

34 With respect to point (d) above, this had already been taken into consideration when the Commissioner decided on the financial penalty.

ENFORCEMENT ACTION BY PERSONAL DATA PROTECTION COMMISSION

35 Given that the Commissioner has found the Organisation in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as he 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 as the Commissioner thinks fit.

36 In assessing the breach and determining the directions to be imposed on the Organisation, the Commissioner took into account the following factors:

Aggravating factors

(a) the personal data of more than 4,000 individuals was at risk of unauthorised access, use and disclosure;

(b) the personal data which was at risk included financial information and was sensitive in nature;

(c) an unauthorised user would have been able to alter a Member's investment parameters, which could have led to actual financial losses;

(d) the Organisation was unable to confirm that Mr J had only accessed and extracted the personal data of two Members;[7]

Mitigating factors

(e) the Organisation did not make reasonable efforts to rectify the vulnerability despite being made aware of it early;

(f) the Organisation voluntarily notified the PDPC of the breach;

(g) the Organisation was generally co-operative and forthcoming in providing timely responses to the Commission during the investigation; and

(h) the Organisation took prompt corrective action to resolve the vulnerability after being alerted to the data breach incident, as well as other remedial measures to improve its Website security.

---

7 The Organisation stated that its "system logging did not capture information required to show when [Mr J] was accessing the other user's account data". It was possible that Mr J had accessed and extracted the account data of countless other Members.

37 Having carefully considered all the relevant factors of the case, the Commissioner has decided to impose a financial penalty of $30,000 on the Organisation. This financial penalty is to be paid within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Bud Cosmetics Pte Ltd

[2019] PDP Digest 351

Coram: Tan Kiat How, Commissioner
Case Number: DP-1704-B0660
Decision Citation: [2019] PDP Digest 351; [2019] SGPDPC 1

Openness Obligation *– Requirement to develop and implement policies and practices and communicate these policies and practices to staff*
Protection Obligation *– Disclosure of personal data – Insufficient security arrangements*
Transfer Obligation *– Failure to ascertain and ensure recipient of personal data outside Singapore is bound by legally enforceable obligations to provide comparable standard of protection*

3 January 2019

1 On 6 April 2017, the Personal Data Protection Commission (the "Commission") received a complaint from an individual (the "Complainant") in relation to the publication of a list of approximately 2,300 of the Organisation's members ("Member List") containing their personal data on the Internet (the "Incident") and commenced investigations thereafter.

2 The Commissioner sets out below its findings and grounds of decision based on the investigations carried out in this matter.

MATERIAL FACTS

3 The Organisation is an organic and natural skincare retailer specialising in natural skin care brands with retail outlets in Singapore and an online store that it operates and manages at www.budcosmetics.com (the "Website"). Since 2007, the Organisation has been collecting customer information for membership registration. At the time of the Incident, all customers who wished to purchase items from the Organisation's Website were required to set up a membership account.

4 As a matter of practice, the Organisation maintained two separate membership databases. The first database was for customers who registered to become members on its Website, which was kept in the SQL database and stored on the host server (the "Online Database"), while the second database was for customers who registered in person at the Organisation's retail outlets (the "Offline Database").[1] The Offline Database was provided by the Organisation's vendor as part of its point-of-sale system. At all material times, the Online and Offline Databases were not consolidated but were kept and updated separately. Personal data extracted from the Offline Databases was not stored in any folders linked to the Website. The Online Database contained approximately 1,132 members in 2012. At the time of the investigation, the Organisation represented that there were approximately 2,457 registered members on the Online Database.

5 As part of its marketing strategy, the Organisation prepared and sent its customers e-newsletters with information about its products and the latest promotional offers. A customer mailing list for each e-newsletter was generated by selecting members' e-mail addresses from both the Online and Offline Databases based on certain criteria. When generating this list, the Organisation would only extract e-mail addresses from both the Online and Offline Databases. It would not extract the other types of personal data and combine the records into a master list; the Organisation confirmed that apart from the e-mail addresses for the purposes of sending out marketing newsletters, it did not combine the datasets from the Online and Offline databases. To reduce the file size of each e-newsletter, the Organisation intentionally kept the images embedded in the e-newsletters in publicly accessible image folders. Once an e-newsletter was sent out, the customer mailing list for that particular e-newsletter would be kept in an archive folder. The image folders and customer mailing lists were managed and generated by the owner of the Organisation.

6 On or around 6 April 2017, the Complainant, who was a member of the Organisation, discovered a URL to the Member List in the search results when she conducted a search using her name on the Internet. The Member List contained the following personal data of approximately 2,300 members:

---

1 At the time of the investigation, the Organisation represented that there were approximately 5,000 registered members on the Offline Database.

(a) name;
(b) date of birth;
(c) contact number;
(d) e-mail address; and
(e) residential address.

7 The Member List was located in the image folder for an e-newsletter that was sent out in 2012 ("2012 Image Folder"). At the time, the 2012 Image Folder was hosted on SmartyHost Pty Ltd's ("SmartyHost") servers based in Australia. However, following a cyberattack incident on SmartyHost's "osCommerce" system in April 2012 ("2012 Cyberattack Incident") and unplanned server outages which resulted in website downtime, the Organisation switched web hosting companies in 2013 and engaged Just Host Inc ("Just Host"), a US-based company with servers located in Provo, Utah.

8 After it was notified of the Incident, the Organisation deleted the Member List from the 2012 Image Folder as well as the e-newsletter image folders created from 2006 to 2016. The Organisation also sought to improve the security of its Website by activating "Sitelock", an add-on feature offered by Just Host which conducts daily scans of its Website for vulnerabilities and malware.

Cause of the Incident

9 Investigations found that search engines were able to access and index the URL to the Member List contained in the 2012 Image Folder because the 2012 Image Folder was unsecured. The Organisation represented that, prior to the notification from the Commission, it was unaware of the existence of the Member List, or how it ended up in the 2012 Image Folder. However, it hypothesised that the Member List may have been inserted into the 2012 Image Folder as a result of the 2012 Cyberattack Incident as that was the only known occasion in 2012 where the Organisation had encountered problems with its Website. In the 2012 Cyberattack Incident, hackers exploited a vulnerability in SmartyHost's osCommerce system to send spam e-mails via the "tell-a-friend" function on the system.

10 Having considered the evidence and findings of the investigation, the Commissioner is not convinced by the Organisation's hypothesis.

The vulnerability of the "tell-a-friend" feature does not appear to be in any way connected to the unauthorised extraction of data from the Online Database. More pertinently, the claim that the Incident had occurred in 2012 seems improbable given that the number of members contained in the Member List exceeded the number of online-registered members in 2012 (when they had only approximately 1,132 members). While the Member List could possibly be a combination of 2012-registered members of both the Online and Offline Databases, it is unlikely to be the case as the Organisation had not combined both Databases (save for the combination of e-mail addresses for the mailing list) or linked the Offline Database to the Website such that an exploitation of the "tell-a-friend" feature could have led to the access of the Offline Database.

FINDINGS AND BASIS FOR DETERMINATION

11 The main issues for determination are:

(a) whether the Organisation complied with its obligations under s 12(*a*) of the Personal Data Protection Act 2012[2] ("PDPA");
(b) whether the Organisation breached s 24 of the PDPA; and
(c) whether the Organisation complied with its transfer limitation obligation under s 26 of the PDPA.

12 There was no question or dispute that the data disclosed in the Member List was "personal data" as defined in s 2(1) of the PDPA as it was clearly possible to identify an individual from that data.

13 In this regard, although the Member List contained personal data that was collected before the PDPA came into full force on 2 July 2014 ("Appointed Day"), as the Organisation continued to use the personal data after the Appointed Day, it was incumbent on the Organisation to take proactive steps to comply with its obligations under the PDPA in respect of not only new personal data that may come into its possession or control but any existing personal data held in its possession or control.[3]

2 Act 26 of 2012.

3 See *Re Social Metric Pte Ltd* [2018] PDP Digest 281 at [10].

14 As the Commissioner highlighted in *Re Social Metric Pte Ltd*[4] at [11]:

> This means that, for example, *if there were no security arrangements previously to protect the existing personal data the organisation was holding, the organisation has a positive duty to put in place security arrangements after the Appointed Day*. It was not enough for the organisation to leave things *status quo*, if this would not enable the organisation to meet the requirements and standards of the Protection Obligation. As provided in s 24 of the PDPA, the security arrangements must be 'reasonable'. [emphasis added]

15 Accordingly, the Organisation was under an obligation to comply with the data protection provisions under the PDPA in respect of both personal data that was collected before and after the Appointed Day.

Whether the Organisation breached section 12(a) of the Personal Data Protection Act

16 Section 12(*a*) of the PDPA imposes an obligation on organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. Organisations are also required to communicate to its staff information about such policies and practices.

17 The Organisation represented that it had a privacy policy on its Website ("Privacy Policy") at the time of the Incident. However, the Privacy Policy (which was last updated in December 2006) only notified customers as to how the Organisation will use and process their personal data and did not set out any procedures or practices as to how the Organisation and its employees should handle and protect the personal data in their possession or under their control.

18 In any case, by the Organisation's own admission, prior to being notified by the Commission, the Organisation was under the impression that the PDPA only prohibited organisations from sending marketing messages to Singapore telephone numbers that were registered with the Do Not Call ("DNC") Registry. The Organisation confirmed[5] that it did not implement any data protection policies or practices in respect of the

4 [2018] PDP Digest 281.

5 See the Organisation's response to the Personal Data Protection Commission's Notice to Produce (10 May 2017) at para 2.8.

personal data in its possession or under its control as it was not aware of its data protection obligations under the PDPA.[6] In response to questions on the Organisation's data protection policies and practices, the Organisation said the questions were "(n)ot applicable as we do not currently have a policy/procedure document. However, we would appreciate any assistance in drafting such a policy document for our staff".

19 For completeness, the investigations found that the Organisation had begun drafting a new data protection policy prior to the Incident in February 2017, when it claimed to be unaware of its data protection obligations. However, on balance, the Commissioner accepts the Organisation's representation that it had only drafted the data protection policy because "*during our research of other major local beauty retailer websites we noticed the section on Data Protection Policy section [sic.] on their websites. Hence we thought we should include a similar detailed policy on ours*". The new data protection policy was only implemented after the Incident in June 2017, when the Organisation launched its new Website.

20 In this regard, it is a trite principle of law that ignorance of the law is no excuse. The Organisation's lack of awareness of its obligations under the PDPA cannot excuse its breach of the PDPA and is not a legitimate defence to a breach.[7] It bears repeating that the development and implementation of data protection policies is a fundamental and crucial starting point for organisations to comply with their obligations under the PDPA. As the Commissioner highlighted in *Re Aviva Ltd*[8] at [32]:

> Data protection policies and practices developed and implemented by an organisation in accordance with its obligations under s 12 of the PDPA are generally meant to increase awareness and ensure accountability of the organisation's obligations under the PDPA.

21 Data protection training is also an effective and necessary mode of communicating the Organisation's policies and practices and is a key aspect of the Openness Obligation under s 12 of the PDPA.[9] Employees will only

---

6 Under Pts III to VI of the Personal Data Protection Act 2012 (Act 26 of 2012).

7 *Re M Stars Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 (at [16]).

8 [2018] PDP Digest 245.

9 See *Re Habitat for Humanity Singapore Ltd* [2019] PDP Digest 200 at [14].

be able to protect personal data if they are first able to recognise when a matter requires data protection considerations. In this regard, the Commissioner agrees with the following observations in the Joint Guidance Note issued by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia:[10]

> Training and general education on privacy are very important. *Our Offices have seen instances where issues were not identified as privacy issues when they should have been. As a result, appropriate steps were not taken to prevent or address privacy breaches. In other cases, we have seen a lack of awareness or appreciation for privacy risks on the part of employees result in the development of products or services that were not compliant with applicable privacy law.* In Alberta, human error is the most common cause of reported breaches resulting in a real risk of significant harm to an individual. Examples include: misdirected faxes and mail, e-mail addresses viewable in mass e-mails, inappropriate disposal of documents, and disclosure of passwords.
>
> *Employees will be able to better protect privacy when they are able to recognize a matter as one that involves personal information protection.*
>
> [emphasis added; internal footnotes removed]

22 However, apart from instructing its employees on the requirements under the DNC provisions of the PDPA,[11] the Organisation did not provide any formalised data protection training for its employees. Accordingly, the Commissioner finds that the Organisation had breached s 12(*a*) of the PDPA given that at the time of the Incident the Organisation did not develop and implement a data protection policy as necessary for it to meet its obligations under the PDPA.

---

10 Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, "Getting Accountability Right with a Privacy Management Program" (April 2012) at p 13.

11 In this regard, the Organisation represented that it had instructed the members of its sales team to ensure that they require customers to indicate if they want to be contacted by the Organisation when they sign up to be a member and to inform the customers that their data will not be sold or offered to any third party. The Organisation also represented that it only sent text messages via SMS to customers whose numbers were not on the Do Not Call Registry.

Whether the Organisation breached section 24 of the Personal Data Protection Act

23 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Member List containing the personal data of the Organisation's online-registered members was located in an image folder that belonged to and was at all material times controlled by the Organisation. Accordingly, the Commissioner finds that the Member List was in the Organisation's possession. The Organisation was also in control of the personal data as it had the ability, right and/or authority to determine what personal data was required to provide its services and the purposes for, and the manner in which it was collected, used and disclosed.[12] Such control was demonstrated when it generated the respective e-newsletter customer mailing lists and when it deleted the Member List upon being notified of the Incident.

24 While the cause of the Incident cannot be determined with certainty after investigations, the fact remains that the Member List was generated and inserted into the 2012 Image Folder. The common law maxim *res ipsa loquitur* applies even though the Organisation showed a clear lack of knowledge of how and when this happened. As the Website administrator, the Organisation was responsible for ensuring the security of the Website such as by conducting periodic penetration testing or vulnerability assessments and ensuring that any vulnerabilities are reviewed and promptly fixed to prevent data breaches. However, by the Organisation's own admission, prior to being informed of the Incident, the Organisation never considered the adequacy of the security of its Website or information technology system ("IT system") and did not put in place any security arrangements to protect the personal data in its possession or under its control. At the time of the Incident, the Organisation had never conducted any vulnerability scans or penetration tests to ensure that its Website was sufficiently protected.

25 As mentioned above, the Organisation was unaware of its Data Protection Obligations under the PDPA at the time of the Incident and

12 The meaning of control as set out in *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 189 at [18].

therefore did not have any policies or procedures in place to guide its employees regarding the collection, use and disclosure of personal data in its possession or under its control. Consequently, the Organisation did not implement any checks and controls to prevent or minimise the risk of unauthorised disclosure of personal data. By way of example, the Organisation failed to implement procedures for the generation of the Member List, use of the Member List for sending e-newsletters and deletion of the Member List after e-newsletters have been sent. Given the Organisation's practice of retaining the publicly accessible e-newsletter image folders for extended periods, proper housekeeping should have been conducted to ensure that all publicly accessible folders did not contain extraneous files, including stray copies of the Member List.

26 As mentioned in the *Guide to Securing Personal Data in Electronic Medium*, managing info-communication technology systems security and risks related to data breaches requires good governance. It is a good practice for organisations to:[13]

> Conduct periodic checks for personal data stored in ICT systems. For personal data that is not required in any form anymore, securely dispose the data (refer to section 8). If there is a need to retain the data but not in identifiable form, e.g. for performing data analytics, consider anonymising the data.

27 In the light of the absence of any security arrangements to protect the personal data from unauthorised disclosure, the Commissioner finds that the Organisation has contravened s 24 of the PDPA.

Whether the Organisation breached section 26 of the Personal Data Protection Act

28 Under s 26 of the PDPA, unless otherwise exempted,[14] an organisation shall not transfer any personal data to a country or territory

---

13 Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017) at para 4.1.

14 A transferring organisation is taken to have satisfied the requirements to ascertain and ensure that the recipient of the personal data outside Singapore is bound by legally enforceable obligations to provide a comparable standard of protection in the situations set out in reg 9(3) of the Personal Data Protection Regulations 2014 (S 362/2014).

outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA. The regulations issued under the PDPA specify the conditions under which an organisation may transfer personal data outside Singapore.

29 In particular, reg 9(1) of the Personal Data Protection Regulations 2014[15] provides that an organisation must take appropriate steps to:

(a) ensure that the transferring organisation will comply with the Data Protection Obligations under the PDPA, in respect of the transferred personal data while it remains in the possession or under the control of the transferring organisation; and

(b) ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations[16] to provide the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

30 In this regard, it was not disputed that the Organisation had engaged SmartyHost and Just Host to host its Website and the Online Database. As mentioned above, SmartyHost was based in Australia and Just Host is based in the US. Both companies had servers located outside Singapore.

31 While personal data collected and transferred overseas before the Appointed Day is not subject to the obligations under the PDPA, a substantial portion of the personal data in the Online Database was collected and transferred to Just Host's servers located in the US after the Appointed Day, and was therefore subject to the Transfer Limitation Obligation under the PDPA. Specifically, the number of members in the Online Database had increased from 1,635 members on 29 December 2014 to 2,457 members on 10 April 2017.

32 By engaging the services of Just Host to host its Website and Online Database on its server in the US, the Organisation had effectively transferred personal data outside Singapore. However, as the Organisation was not aware of the transfer limitation requirement under the PDPA,

15 S 362/2014.

16 As defined under reg 10 of the Personal Data Protection Regulations 2014 (S 362/2014).

the Organisation admitted that it did not ask or even consider the location of the web hosting company's servers to be a relevant factor when it engaged Just Host to provide web hosting services. The Organisation therefore failed to undertake the most fundamental step of considering whether US federal and state laws provided protection comparable to the PDPA. It is not necessary for the Commissioner to venture any opinion whatsoever on the issue of whether US law provided comparable protection in order to find that the Organisation, having been ignorant of its obligation to do so, had in fact failed to undertake the most fundamental step of considering this issue. This omission is sufficient, *ipso facto*, to put the Organisation in breach of s 26 of the PDPA.

33 Had the Organisation undertaken the fundamental step of considering whether US law provided comparable protection, it could have arrived at two possible conclusions. First, it may decide that there is no further requirement for it to impose any additional safeguards by contract as it concluded that US law provided comparable protection. Second, it may decide that there are areas that US law does not provide comparable protection and it may then impose contractual obligations on Just Host to ensure that it provided a standard of protection comparable to the PDPA in respect of the personal data transferred. Needless to say, the Organisation never reached this set of considerations since it omitted to even undertake the most fundamental step.

34 In this regard, organisations that choose to engage IT vendors that are either located overseas or have servers located outside Singapore are reminded of their obligations under s 26 of the PDPA. If the personal data of individuals has to be transferred from Singapore to the overseas destination, organisations will need to ascertain whether and ensure that the recipient of the personal data outside Singapore is bound by legally enforceable obligations to provide the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

35 Therefore, by the Organisation's own admission, the Commissioner finds that the Organisation failed to discharge its duties under s 26 of the PDPA.

Representations

36 The Organisation made representations for a reduction in the quantum of the financial penalty as set out below at [37(a)] on the basis that the retail industry is facing a financial downturn. The financial information adduced by the Organisation to justify its request did not show any significant drop in income. Having duly considered the matters raised in the representations, the Commissioner has decided to maintain his decision on the quantum of the financial penalty.

THE COMMISSIONER'S DIRECTIONS

37 Having found that the Organisation is in breach of ss 12(*a*), 24 and 26 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as it deems fit to ensure compliance with the PDPA:

(a) to pay a financial penalty of S$11,000 within 30 days from the date of this direction, failing which, interest at a rate specified in the Rules of Court in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full;

(b) to engage duly qualified personnel to conduct a security audit of its Website and IT system and furnish a schedule stating the scope of risks to be assessed and the time within which a full report of the audit can be provided to the office of the Commissioner within 30 days from the date of this direction;

(c) to develop an IT security policy to guide its employees on the security of personal data on its Website and IT system within 60 days from the date of completion of the above security audit; and

(d) to implement a training policy for employees of the Organisation handling personal data to be trained to be aware of, and to comply with, the requirements of the PDPA when handling personal data; and to require all employees to attend such training within 90 days from the date of this direction.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re AIG Asia Pacific Insurance Pte Ltd and another

[2019] PDP Digest 363

Coram: Tan Kiat How, Commissioner
Case Number: DP-1702-B0537
Decision Citation: [2019] PDP Digest 363; [2019] SGPDPC 2

Data intermediary *– Data intermediary may be in control of personal data*
Data intermediary *– Obligations of data intermediary and organisation which engages a data intermediary*
Definition of "control"
Protection Obligation *– Disclosure of personal data – Insufficient administrative security arrangements*

3 January 2019

BACKGROUND

1 Today's leading companies are approaching outsourcing in innovative ways to activate, create, integrate and amplify business value. Outsourcing is expected to see growth across all functions, particularly in IT, finance and human resource.[1] This will correspondingly result in an increase in the volume of data processing activities that is outsourced by organisations to data intermediaries.

2 It is, therefore, crucial that data intermediaries and the organisations that engage them understand their respective obligations and those of the other party in this data processing relationship. This matter aims to shed some light in this regard and address the following issues:

(a) whether a data intermediary may have control of the personal data that it processes on another organisation's behalf; and

1 Deloitte, "2016 Global Outsourcing Survey: Outsourcing Accelerates Forward" (June 2016).

(b) if yes, in what circumstances would the data intermediary have such control and whether as a result of this; and

(c) what, if any, are the obligations that the engaging organisation continues to have where the data intermediary is in control of the personal data.

3 On 21 February 2017, AIG Asia Pacific Insurance Pte Ltd ("AIG") informed the Personal Data Protection Commission (the "Commission") regarding an incident with its printing vendor, Toppan Forms (S) Pte Ltd ("Toppan"). Toppan mailed out 87 policy renewal letters ("Policy Renewal Letters") addressed to the respective individual AIG policyholders ("Affected Customers") enclosing incorrect business reply envelopes (the "Incident"). The incorrectly enclosed business reply envelope was addressed to Tan Chong Credit Pte Ltd ("Tan Chong Credit") instead of AIG.[2]

4 The Commissioner makes the following findings:

(a) AIG did not breach s 24 of the Personal Data Protection Act 2012[3] ("PDPA"); and

(b) Toppan breached s 24 of the PDPA.

MATERIAL FACTS

5 AIG is one of the leading general insurance companies in Singapore.

6 The Incident occurred on or around 10 October 2016 and was discovered by AIG on 2 November 2016 when it contacted an Affected Customer to invite him to renew his motor insurance policy. The Affected Customer informed AIG of the incorrectly inserted business reply envelope.

7 The Policy Renewal Letters sent to the Affected Customers enclosed two Motor Insurance Renewal Notices. The first notice was to be completed if the Customer wished to also extend the insurance to cover home protection besides the motor insurance. If the Affected Customer only wished to renew the motor insurance, the Customer would only complete the second notice. The Affected Customer was to then return either one of the completed notices to AIG. This could presumably be done

2 Tan Chong Credit Pte Ltd is one of AIG Asia Pacific Insurance Pte Ltd's scheme partners.

3 Act 26 of 2012.

either by inserting the completed notice in the enclosed business reply envelope or by way of fax as the Organisation's fax number was provided.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

8 The personal data in each renewal form comprised:

(a) The personal data printed on the first page of both Motor Insurance Renewal Notices which comprised an Affected Customer's name, address, make of vehicle together with registration number, hire purchase company (if any), motor policy number, premium payable, excess as well as renewal and expiry dates (the "Printed Personal Data").

(b) In addition, customers were also required to fill in the second page of the relevant Motor Insurance Renewal Notice to update AIG of the customers' marital status, identification number or passport number, address, contact number, *etc*, and input payment details such as credit card number, card holder's name, and card expiry date (collectively, the "In-filled Personal Data").

Printed Personal Data and In-filled Personal Data are collectively referred to as "Personal Data" in this decision.

9 It is not disputed that the Personal Data in the renewal forms constitutes "personal data" as defined in s 2(1) of the PDPA.

10 There is also no dispute that the PDPA applies to AIG and Toppan as they both fall within the PDPA's definition of "organisation".

11 The issues to be determined by the Commissioner in this case are as follows:

(a) whether Toppan was a data intermediary for AIG;

(b) whether AIG had complied with its obligations under s 24 of the PDPA; and

(c) whether Toppan had complied with its obligations under s 24 of the PDPA.

Toppan was a data intermediary

12 Toppan, pursuant to an agreement dated 1 March 2006 and supplemented by Addendum No 1 dated 24 June 2014 (collectively, the "Agreement"), agreed to provide printing, collation and delivery services for AIG. This would have included printing the Policy Renewal Letters and the Motor Insurance Renewal Notices which included the Printed Personal Data. To perform this work, Toppan would have had to record, hold and retrieve the Printed Personal Data, thereby processing personal data on behalf of AIG. Toppan would also have caused the Affected Customers to transmit the Personal Data through the customers use of the business reply envelopes Toppan had enclosed with the Policy Renewal Letters to return the notices.

13 In the circumstances, the Commissioner finds that Toppan was engaged to carry out activities of "processing" personal data on behalf of AIG as defined in s 2(1) of the PDPA. Toppan was therefore acting as a data intermediary of AIG.

Elements of section 24 under the Personal Data Protection Act

14 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.

15 The obligation to make reasonable security arrangements does not attach unless the organisation is in possession or control of personal data.

AIG and Toppan had possession of the Printed Personal Data

16 AIG was in possession of the Printed Personal Data. First, AIG had the Printed Personal Data of each of the Affected Customers on record as each of them had an existing relationship with AIG. Second, it was AIG who provided Toppan with the Printed Personal Data.

17 Toppan was in possession of the Printed Personal Data from the moment it received the data from AIG.

The meaning of "control" in the Personal Data Protection Act

18 While there is no definition of "control" in the PDPA, the meaning of control in the context of data protection is generally understood to cover "the ability, right or authority to determine (a) the purposes for; and/or (b) the manner in which personal data is processed, collected, used or disclosed".[4]

19 The organisation which engages a data intermediary to process personal data on its behalf (in this case AIG) will always have overall control of the purposes for which, and manner in which, personal data is processed, collected, used or disclosed.

20 A data intermediary is unlikely to have control over the purposes for which personal data is processed, collected, used or disclosed. If a data intermediary has control over the purposes for the collection, use or disclosure of the personal data, it is likely to be processing personal data on its own behalf rather than on behalf of another organisation.

21 A data intermediary, however, may be in control over the manner in which personal data is processed, collected, used or disclosed from a practical perspective, especially where the data intermediary is in the best position to determine the specific manner in which the personal data is processed, collected used or disclosed and the organisation defers to the data intermediary on how best to process, collect, use or disclose the personal data because of the data intermediary's expertise in the processing of personal data.

22 In the current business environment, where the outsourcing of data processing is increasingly prevalent and has led to a well-developed business process outsourcing industry, the reality is that these data intermediaries have specialised knowledge, skills and tools, including in the area of data processing, that the organisations which engage them may not have. The fact is that organisations no longer engage data intermediaries just to bring costs down but increasingly because of their expertise and resources available in specific areas, including the handling personal data. In these circumstances, such data intermediaries are likely to be in the best position to advise or determine the manner in which personal data is processed,

4 See *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 189 at [18].

collected, used or disclosed and the relevant security measures to be implemented to protect the personal data being processed.

23 In addition, s 4(2) read together with s 24 of the PDPA supports the view that a data intermediary may be in control of personal data. Pursuant to s 4(2), data intermediaries are subject to s 24 of the PDPA, which obliges the data intermediary to "protect personal data in its possession or under its control". A data intermediary may, therefore, be in possession of, and/or in control of, personal data.

24 This is consistent with the purpose of the PDPA in recognising both the protection of personal data and the need for organisations to collect, use and disclose personal data for legitimate purposes.[5] A data intermediary that has the relevant expertise, knowledge and/or tools in handling and protecting personal and has been trusted with determining the manner in which personal data is processed is in the best position to protect that personal data; even if the data intermediary is not in possession of the personal data it ought to be responsible for the protection of such personal data.

AIG had control of the Personal Data as a whole

25 AIG was in control of the Personal Data as a whole, including the In-filled Personal Data. Similar to *Re AIG Asia Pacific Insurance Pte Ltd*,[6] in this case, AIG determined what personal data it required to provide its services and the purposes for which the Personal Data was processed, collected, used and disclosed. In particular, AIG was in a position to decide, and did in fact do so, that in order to provide a better experience for customers when renewing their policies, the Printed Personal Data was pre-filled in the opening section of the renewal form. With respect to the In-filled Personal Data, AIG was responsible for determining what personal data was required from its customers and the purposes for which the In-filled Personal Data was processed, collected, used and disclosed. Therefore, in so far as the Affected Customers were returning the completed notices with the Personal Data, such Personal Data was within AIG's control at the material time.

---

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

6 [2019] PDP Digest 189 at [20] and [24].

Toppan also had control of the Personal Data as a whole

26 Toppan indicates on its website www.toppanforms.com/eng/about_us.html that the Toppan Forms (Hong Kong) Group (of which Toppan is part of) "has been providing one-stop total information management solutions to help our clients find better ways to handle information asset".

27 In fact, Toppan touts its data management expertise in various places on its website, stating that:

> Data Management Services at Toppan Forms is *a high security business process outsourcing service specializing in data handling*. ISO 9001:2008 Quality Management Certificate and ISO 27001:2005 Information Security Management Systems Certification guarantee that our operations are up to certified international standards. We help you maximize the value of data asset *while minimizing handling cost and data leakage risk*.
>
> We provide a wide range of data management services from data print and business mailing service to document digitization.
>
> [emphasis added]

28 It is clear from the above that Toppan does not see itself merely as a vendor that prints forms and mails them out but rather a specialised business process outsource service with the value proposition that it not just prints forms but ensures data security. This is consistent with cl 3.3 of Addendum No 1 dated 24 June 2014, which is part of the Agreement, wherein Toppan:

> [R]epresents and warrants to AIG that it has and will continue to have *industry best practice administrative, technical, and physical safeguards* in place to ensure the security and confidentiality and protect against the unauthorised or accidental destruction, loss, alternation (sic), use or disclosure of Client Data and other records and Information of AIG's customers or employees, to protect against anticipated threats or hazards to the integrity of such information and records. [emphasis added]

29 Client Data is defined in the Addendum to mean "any 'personal data' as defined under the Personal Data Protection Act 2012 (Act 26 of 2012), all subsidiary legislation, guidelines, and notices as amended or issued thereunder from time to time".

30 Toppan is no ordinary form-printing and mailing vendor and instead recognises itself as having expertise in the area of data protection and data security in relation to its form printing and mailing outsourcing services.

31 As explained above, such organisations are likely to have control over the means in which personal data is processed, collected, used or disclosed. In this regard, the investigations revealed that Toppan had control over the systems, processes and practices implemented to process the Personal Data in the notices from the time of receipt of the notices from AIG, to the enveloping of the Policy Renewal Letters, to the mailing out of these letters, and up to the onward transmission of the notices by AIG's customers by way of returning the notices in the business reply envelopes.

32 Toppan was solely responsible for its enveloping process during which business reply envelopes were enclosed with the Policy Renewal Letters, and was, therefore, in control of directing the manner and mode in which Affected Customers returned the completed renewal forms (and the Personal Data contained therein). These processes were not dictated by AIG and AIG did not have input in how these processes were drawn up.

33 Given the above, Toppan was, like AIG, also in control of the Personal Data as a whole. This is given Toppan's control over the manner in which the Personal Data was handled and the processes it put in place to print, envelope and mail out the Policy Renewal Letters comprising the Personal Data.

Whether AIG complied with its obligations under section 24 of the Personal Data Protection Act

34 AIG had the same obligation in respect of personal data processed on its behalf and for its purposes by Toppan as if the personal data were processed by AIG itself.[7]

35 Based on the investigations, the Commissioner finds that AIG had complied with its obligations under s 24 of the PDPA.

36 In order to take into account obligations under the PDPA, AIG supplemented its agreement with Toppan dated 1 March 2006 with Addendum No 1 dated 24 June 2014. Under cl 3.2 of the Addendum,

7 See s 4(3) of the Personal Data Protection Act 2012 (Act 26 of 2012).

the covenants made by Toppan with respect to "Client Data"[8] included the following:

(a) to inform itself regarding, and comply with, AIG's privacy policies and all applicable privacy laws, including the "Privacy Laws";[9]

(b) to maintain adequate administrative, technical and physical safeguards to ensure the security and confidentiality of the "Client Data", protect against any anticipated threats or hazards to the security or integrity of the "Client Data", and protect against unauthorised access to, use of or disclosure of "Client Data".

37 The Incident, as will be explained below, was a result of a gap in Toppan's enveloping process where the necessary checks were not carried out and AIG had no part to play in the actual breach. While this does not automatically excuse AIG from a finding of a s 24 breach, the Commissioner is of the view that it would not be reasonable to have required AIG to implement any further security arrangements given the circumstances in this case.

38 Toppan's standard operating procedure, which was updated in January 2017, set out the necessary checks that Toppan had put in place in respect of the printing, enveloping and mailing of the Policy Renewal Letters. This document, if followed, would have prevented the Incident. Of course, AIG could have audited Toppan's enveloping process in a "live" environment to confirm that the relevant checks in respect of ensuring the correct business reply envelope was enclosed were being carried out. However, given Toppan's credibility and expertise in the area of data

8 Defined in the Addendum as "any 'personal data' as defined under the Personal Data Protection Act 2012 (Act 26 of 2012), all subsidiary legislation, guidelines, and notices as amended or issued thereunder from time to time and any information regarding AIG's (and/or its Affiliates) clients or prospective clients received by (Toppan) in connection with the performance of its obligations under the Agreement".

9 Defined in the Addendum as "any Singapore laws, rules or regulations relating to personal information or collection, use, storage, disclosure or transfer of personal information, including the Personal Data Protection Act 2012 (Act 26 of 2012), all subsidiary legislation, guidelines, and notices issued thereunder from time to time, as may be amended from time to time".

protection management and data security and Toppan's contractual obligation to maintain industry best practices (as opposed to mere compliance with the PDPA) in implementing security arrangements, any requirement to audit such a seemingly minor part of Toppan's complete process would appear to amount to a requirement for AIG to micromanage its data intermediaries' activities. There may be circumstances where such micromanagement is required, but based on the facts here, this case is not one of those circumstances.

39 Given the circumstances, the Commissioner does not find AIG to be in breach of s 24 of the PDPA.

Whether Toppan complied with its obligations under section 24 of the Personal Data Protection Act

40 As AIG's data intermediary, Toppan had an obligation to put in place reasonable security arrangements to protect the Printed Personal Data and In-filled Personal Data which was in its possession and/or under its control.[10]

41 At the material time, Toppan's standard operating procedure for enveloping was as follows ("Toppan's Enveloping Process"):

(a) Step 1 – A supervisor checks for the use of correct stationery including the use of correct business reply envelopes, quantity of letters to be printed and the appearance of the printout.

(b) Step 2 – The enveloping employee manually envelopes the printed letters according to a checklist. The enveloping employee signs off as first checker after checking for correct page sequence and dirty or misaligned prints.

(c) Step 3 – The supervisor conducts a quality control check by ensuring the addressee's name and address are visible in the envelope window and that the number of letters enveloped tallies with the checklist. The envelope content is not checked. The supervisor signs off as second checker.

(d) Step 4 – A manager does a sampling check on content. The manager must check content of the first five, the last five and

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

another five randomly chosen envelopes. The manager then signs off.

(e) Step 5 – The packing employee tallies the number of envelopes with the checklist before sealing and sending the envelopes for mailing.

42 The investigations found that Toppan's enveloping employee inserted the incorrect business reply envelope because it looked similar to the correct reply envelope and failed to submit the unsealed envelopes for the supervisor and manager to conduct their respective checks. Also, Toppan's staff who packed the envelopes for mailing did not check for signatures of the supervisor and manager before sealing and mailing the enveloped Policy Renewal Letters.

43 Toppan's Enveloping Process fell far short of the standard protection required for the processing of the Personal Data, and amounted to weak internal work process controls:

(a) the enveloping employee was able to bypass the relevant checks during the Enveloping Process undetected;

(b) no specific instruction was given to the enveloping employee to check that the correct business reply envelope is inserted; and

(c) the packing employee was not instructed to check for signatures of the supervisor and manager before sealing and mailing the enveloped Policy Renewal Letters.

44 Toppan was processing a significant volume of personal data on behalf of one of the leading general insurance companies in Singapore. It was therefore incumbent on Toppan to put in place reasonable security arrangements to protect this personal data. In this regard, Toppan was fully aware of its obligations, and had in fact made specific warranties to implement industry best practice security arrangements with respect to its processing of Personal Data as discussed at [28] above.

45 The data breach could have been avoided if simple additional steps had been included in Toppan's Enveloping Process, for example:

(a) Toppan could have required notification to the assigned supervisor and manager before the start of each enveloping job. This would have made it less likely for their respective sampling checks to have been bypassed, as happened in the Incident.

(b) Toppan could have required its packers to have sight of the signatures of the supervisor and manager before sealing and mailing the enveloped Policy Renewal Letters.

(c) As part of the job instructions for each enveloping job, Toppan could have required its employee to check that the correct business reply envelope is inserted.

46 For the reasons above, the Commissioner finds Toppan in breach of s 24 of the PDPA.

REMEDIAL ACTION TAKEN BY TOPPAN

47 Toppan took the following remedial actions after it was notified of the Incident:

(a) the random sampling size for content checks was increased to 30%;

(b) the packers are required to inform the manager or supervisor if signatures of the relevant supervisor and manager are not on the accompanying checklist;

(c) the relevant supervisor and manager are required to track the number of enveloping jobs and ensure all enveloping jobs are checked and signed off by them before the batch is sent to the packers;

(d) employees are to be reminded during daily meetings and monthly Work Improvement Meetings to strictly follow the standard operating procedure for enveloping works; and

(e) a stern warning was given to the employee responsible for the Incident.

THE COMMISSIONER'S DIRECTIONS

48 Given the Commissioner's findings that Toppan is in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to issue Toppan such directions as it deems fit to ensure compliance with the PDPA. This may include directing Toppan to pay a financial penalty of such amount not exceeding S$1m.

49 In assessing the breach and determining the directions, if any, to be imposed on Toppan in this case, the Commissioner also took into account the following mitigating factors:

(a) Toppan co-operated fully with the investigations;
(b) Toppan took prompt remedial action to prevent future breaches of a similar nature from recurring; and
(c) the impact of the data breach was limited. Only one Affected Customer used the incorrectly inserted business reply envelope.

50 Having considered all the relevant factors of this case, the Commissioner hereby directs Toppan to pay a financial penalty of S$5,000.00 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[11] in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

11 Cap 322, R5, 2014 Rev Ed.

Grounds of Decision

Re Singapore Health Services Pte Ltd and others

[2019] PDP Digest 376

Coram: Tan Kiat How, Commissioner
Case Number: DP-1807-B2435
Decision Citation: [2019] PDP Digest 376; [2019] SGPDPC 3

Data intermediary *– Obligations of organisations and data intermediaries*
Personal data *– Personal data in medical records – Stronger controls needed to protect medical data*
Protection Obligation *– Unauthorised access to, and disclosure of, personal data – Insufficient technical and administrative security arrangements*

14 January 2019

1 This case concerns the worst breach of personal data in Singapore's history. In an unprecedented cyberattack on the Singapore Health Services Pte Ltd's ("SingHealth") patient database system, the personal data of some 1.5 million patients and the outpatient prescription records of nearly 160,000 patients were exfiltrated in a cyberattack (the "Data Breach").

2 Following the announcement on 20 July 2018 by the Ministry of Communications and Information and the Ministry of Health ("MOH"), a four-member Committee of Inquiry ("COI") was convened by the Minister for Communications and Information to look into the cyberattack, find out what went wrong and recommend ways to better safeguard critical systems. The COI concluded its hearings and submitted its report on 31 December 2018 to the Minister-in-charge of Cyber Security. The public report of the COI's findings was released on 10 January 2019 ("Public COI Report").

3 Soon after the announcement of the Data Breach, the Personal Data Protection Commission (the "Commission") received several complaints from members of the public regarding the Data Breach. The Commission commenced its investigations thereafter ("Investigation"). The organisations involved were SingHealth and Integrated Health Information Systems Pte Ltd ("IHiS").

4 SingHealth and IHiS (collectively, the "Organisations") agreed to cooperate with the Commission to expedite the Investigation and determination of liability and for the Commission to issue such directions that it deems fit on the basis of the Organisations' representations. In this regard, the Organisations voluntarily and unequivocally admitted to the facts as set out in this decision and accepted the Commissioner's findings in this decision.

5 The Commissioner's findings and grounds of decision, which are based on the Organisations' representations, are set out below. Additionally, the Organisations have agreed to incorporate references to relevant sections of the Public COI Report relating to their representations and the factual issues addressed therein. Accordingly, the Commissioner has referred to some parts of the Public COI Report in the grounds of decision.

MATERIAL FACTS

6 The following chronology and summary of admitted facts were provided by IHiS and SingHealth in their submissions. SingHealth is one of three healthcare clusters in the Singapore public healthcare sector. In Singapore, public healthcare institutions ("PHIs") are grouped into clusters ("Clusters"). IHiS and SingHealth are wholly-owned subsidiaries of MOH Holdings Pte Ltd ("MOHH"), the holding company through which the Singapore Government owns the corporatised institutions in the public healthcare sector. MOH determines the policies and structures within the healthcare sector.

7 The SingHealth Cluster comprises Singapore General Hospital ("SGH"), Changi General Hospital, Sengkang General Hospital, KK Women's and Children's Hospital, National Cancer Centre, National Dental Centre Singapore, National Heart Centre Singapore, National Neuroscience Institute, Singapore National Eye Centre, SingHealth Community Hospitals and SingHealth Polyclinics.[1] SingHealth's primary function is the provision of healthcare services.

1 Polyclinics in Bedok, Bukit Merah, Marine Parade, Outram, Pasir Ris, Punggol, Sengkang and Tampines, as well as Bright Vision Hospital. Two other polyclinics in Queenstown and Geylang used to be under SingHealth.

8 IHiS is the central national IT agency for the public healthcare sector in Singapore. IHiS is also the MOH-designated Sector Lead for the healthcare sector for liaising with the Cyber Security Agency of Singapore ("CSA"). Prior to 2008, PHIs were responsible for their own IT functions and strategy. In July 2008, IHiS was established by MOH to centralise all of the IT functions and capabilities of the PHIs (including IT staff) in a single entity, which would support all the PHIs. IHiS also assumed responsibility for the development and maintenance of the Clusters' IT systems (including SingHealth). The objectives of centralisation were to, *inter alia*: (a) enable better alignment of IT strategies and integration of patient care across PHIs, and (b) reduce the cybersecurity vulnerabilities inherent in a varied and fragmented IT landscape.

9 IT resources in the public healthcare sector were further consolidated in November 2016, when MOHH's Information Systems Division ("ISD") was merged with IHiS. With this merger, national healthcare systems which were originally managed by ISD came under IHiS's management as well. Each Cluster, SingHealth not excepted, has a Group Chief Information Officer ("GCIO") and a Cluster Information Security Officer ("CISO"). Pursuant to the public healthcare sector policy, Healthcare IT Security Policy and Standards (Version 3.0) ("IT-SPS"), the GCIO provides leadership and direction for the Cluster's IT security program, including the establishment and maintenance of the program objectives, strategy, and short- and medium-term activities such as aligning strategic IT initiatives with the Cluster's business objectives. The GCIO is assisted by the CISO, who is charged with security oversight for the Cluster. The CISO reports to the GCIO directly on security matters.

10 Upon the formation of IHiS in 2008, the employment of the majority of IT staff across the Clusters at the time, including SingHealth, was transferred to IHiS. Since then, IHiS has been responsible for hiring and managing IT personnel at both the management and operational level for functions such as general management, maintenance and security management. However, IHiS designates some IT personnel to be redeployed to the Clusters to be responsible for providing leadership and direction for the IT security program as well as executive management oversight of the local Cluster IT systems. In the present case, the SingHealth GCIO and SingHealth CISO are employed by IHiS but

deployed to SingHealth to serve the IT needs of SingHealth. The staff of the SingHealth GCIO Office[2] that supports the SingHealth GCIO and carries out, among other duties, operational and security oversight of SingHealth's IT systems are also deployed by IHiS to SingHealth.[3]

11 GCIOs are accountable to their Clusters for the Chief Information Officer ("CIO") services they provide, such as IT capability development, systems resiliency and security. In SingHealth, the GCIO reports to SingHealth management via the SingHealth Deputy Group Chief Executive Officer (Organisational Transformation and Informatics) ("DGCEO (OT&I)"). The SingHealth GCIO is also concurrently accountable to the Chief Executive Officer ("CEO") of IHiS for the quality of the CIO services provided to the Cluster.[4]

12 IHiS has a centralised Delivery Group which manages the day-to-day operations and technical support, maintenance and monitoring of the entire SingHealth IT system, including the Sunrise Clinical Manager system ("SCM"), as well as the other Clusters' IT systems. The IHiS Delivery Group also covers the security aspects of the Clusters' IT systems and plays a supportive role in rolling out security measures. Within the IHiS Delivery Group, the Security Management Department ("SMD") covers a broad portfolio of IT security in the Clusters. The SingHealth GCIO Office relies on the IHiS Delivery Group for its technical expertise on security and operational matters.

---

2 The SingHealth Group Chief Information Officer Office has a staff strength of 50 members who are Integrated Health Information Systems Pte Ltd employees.

3 The SingHealth Group Chief Information Officer Office is made up of staff deployed from Integrated Health Information Systems Pte Ltd who are mostly IT directors from SingHealth's institutions that carry out management oversight roles of the institutions' IT operations.

4 The CEO of Integrated Health Information Systems Pte Ltd sets the key performance indicators of the SingHealth Group Chief Information Officer ("GCIO") and GCIO Office, namely capability development, resiliency and cost effectiveness.

SingHealth's electronic medical record system

13 SingHealth uses SCM, an electronic medical record ("EMR") software solution from Allscripts Healthcare Solutions, Inc ("Allscripts"). Through SCM, there is a single enterprise-wide EMR containing real-time patient data. SCM is vital to SingHealth's operations and is actively used by SingHealth staff in patient care and management.

14 SCM was implemented by SingHealth in 1999. The IHiS Delivery Group took over the management of SCM in 2008, when the IT team at SingHealth responsible for managing SCM was transferred to IHiS. The SCM database contains patient medical records, including the following types of personal data concerning SingHealth's patients:

(a) patient particulars (*eg*, name, National Registration Identification Card numbers ("NRIC"), address, gender, race and date of birth);
(b) clinical episode information (*eg*, A&E, inpatient, outpatient);
(c) orders (*eg*, laboratory, radiology, cardiology, medication, nursing);
(d) results (*eg*, of diagnostic tests and orders);
(e) clinical documentation (*eg*, from doctors, nurses, rehabilitation);
(f) vital signs (*eg*, blood pressure, pulse);
(g) medical alerts and allergies;
(h) diagnosis and health issues;
(i) vaccination details;
(j) discharge summaries;
(k) medical certificates; and
(l) outpatient medication dispensed (with associated patient demographics).

15 As of July 2018, the SCM database contained patient data of over 5.01 million unique individuals.

16 The SCM IT network is spread across two sectors:

(a) the SingHealth network, which includes infrastructure in the SingHealth campus; and
(b) the Healthcare-Cloud ("H-Cloud") at the Healthcare Data Centre ("HDC"). H-Cloud was set up in 2014 by IHiS as part of a data centre consolidation exercise across the PHIs as well as for IHiS to leverage cloud technologies in serving the PHIs.

17 Before June 2017, the SCM system (which includes the Citrix servers hosting the SCM client application and the SCM database servers) was located at SingHealth's SGH campus. The Citrix servers serve as middleware (*ie*, the bridging between an operating system or database and applications on a network) supporting many applications used in SingHealth's daily operations, including the SCM client application. Citrix servers allow for virtualisation of the SCM client application without the need for a local installation on the user's workstation. There is no transactional data that flows directly between the user's workstation and the SCM database. Users can only view screen images of the SCM client application.

18 The SCM system at SGH (*ie*, both the SCM database servers and Citrix servers) was migrated to be hosted in H-Cloud in June 2017. Since June 2017, a typical SingHealth user would access the SCM system in the following manner:

(a) From the user's workstation, the user launches a virtual SCM client application hosted on the H-Cloud Citrix servers. The application will require the user to enter his unique user credentials to log in to the SCM client application. The user credentials are sent through the Citrix server to the SCM security server for authentication.

(b) Upon successful authentication, the user will be able to access information on the SCM database corresponding to the user's designated role and responsibilities.

Data Breach

19 Between 27 June and 4 July 2018, the personal data of 1,495,364 unique individuals were illegally accessed and copied from the SCM database. The illegal access and copying was limited to a portion of the SCM database, and only in respect of the following personal data:

(a) the names, NRIC numbers, addresses, gender, race, and dates of birth ("Patient Particulars") of 1,495,364 SingHealth patients; and

(b) the outpatient dispensed medication records ("Dispensed Medication Records") of 159,000 patients (which is a subset of the full set of illegally accessed personal data).

Sequence of events

20 Based on forensic investigations by IHiS and CSA, the attacker gained initial access to the SCM network in August 2017 by infecting a user's workstation. This was likely through an e-mail phishing attack, which led to malware and hacking tools subsequently being installed and executed on the user's workstation.

21 Once the attacker established an initial foothold through the affected workstation, the attacker used customised malware to infect and subsequently gain remote access to and control of other workstations between December 2017 and May 2018. From these compromised workstations, the attacker was able to gain access to and control of two user accounts: a local administrator account, and another service account (a special user account that applications or services use to interact with the operating system) ("Compromised Accounts"):

(a) The local administrator account was a dormant account not ordinarily used for day-to-day operations and was originally created as a back-up account for use by administrators. This account was secured with an easily deduced password ("P@ssw0rd").

(b) The service account was also a dormant account with full administrative privileges. This account was secured with a password which was self-generated during the installation of the services.

22 Through these Compromised Accounts, the attacker was able to gain access to and control of the Citrix servers located at SGH ("SGH Citrix Servers"). IHiS had planned to decommission these SGH Citrix servers following the migration of the SCM database and the Citrix servers to H-Cloud in June 2017 but the SGH Citrix Servers remained operational and part of the SCM network while the decommissioning process was ongoing because the SGH Citrix Servers were still hosting other applications which were either planned for migration to H-Cloud or decommissioning by FY 2018.

23 While the attacker had managed to log in to the SGH Citrix Servers, which gave it a direct route to the SCM database, the attacker still did not have the credentials that would have enabled it to log in to the SCM database. As such, between end-May and mid-June 2018, the attacker made multiple failed attempts to access the SCM database using invalid

credentials, or accounts that had insufficient privileges to gain access to the SCM database.

24 On 11 June 2018, an IHiS database administrator from the IHiS Delivery Group discovered the multiple failed attempts to log in to the SCM database. She noticed that some user IDs were used on separate occasions to log in to the SCM database, but they could not log in because they were non-existent user IDs or were not granted access. One of the user IDs belonged to a domain administrator from the IHiS Systems Management Department but she verified that he had not made any attempts to log in to the database.

25 More attempts to log in to the database were made on 12 and 13 June 2018. One of the user IDs used was the same as those used on 11 June 2018. It became clear to her on 13 June 2018 that the failed attempts to log in were evidence of someone attempting to gain unauthorised access to the database. On 13 June 2018, a few members of the staff from the IHiS Delivery Group met with the SMD over these login attempts. A chat group was created; members included the Security Incident Response Manager ("SIRM"), the SingHealth CISO and members of the SMD.

26 On 26 June 2018, the attacker managed to obtain login credentials for the SCM database from the H-Cloud Citrix server. CSA assessed that there was an inherent coding vulnerability in the SCM client application which allowed the attacker to retrieve the SCM database login credentials from the H-Cloud Citrix server. These credentials were then used to access the SCM database using one of the compromised SGH Citrix Servers.

27 Between 27 June and 4 July 2018, the attacker used the stolen SCM database login credentials to access and run numerous bulk queries from one of the compromised SGH Citrix Servers on the SCM database. Data that was illegally accessed and copied through such queries was then exfiltrated by the attacker through the initial compromised workstations to the attacker's overseas Command and Control ("C2") servers.

28 Suspicious circumstances were observed by staff of the IHiS Delivery Group who were not members of the SMD. They brought their suspicion to the attention of individual personnel from IHiS' Security Incident Response Team ("SIRT"), which is part of the SMD. One of the personnel thus notified was the SIRM. The staff in the IHiS Delivery Group had reported the suspicious circumstances as they suspected that there was something amiss. While the matter was referred to the SMD, the SIRT was

not formally activated at any point. This was not in accordance with IHiS's Healthcare IT Security Incident Response Framework, version 2.1 ("SIRF") and IHiS's Cluster IT Security Incident Response SOP, version 1.0 ("IR-SOP").

29 On 4 July 2018, an IHiS Assistant Lead Analyst from the IHiS Delivery Group supporting SCM observed alerts generated by a performance monitor which was programmed to monitor database queries. He commenced investigations into the unusual queries on the SCM database. When the Assistant Lead Analyst was unable to trace the user launching the queries or make sense of the queries on his own, he alerted his colleagues from the IHiS Application, Citrix and Database teams to assist in the investigations. An automated script was then developed and implemented on the SCM database by the Assistant Lead Analyst together with an IHiS Database Administrator from the IHiS Delivery Group to terminate the queries, log the queries and send alerts to them when such queries are identified. The Citrix Team Lead also took steps to block access to the SCM database from any SGH Citrix Server and submitted requests to create firewall rules to block all connections to the SCM database originating from any SGH Citrix Server. Collectively, these efforts stopped the further exfiltration of data from the SCM database.

30 The SIRM and the SingHealth CISO were both aware of the suspicion of attack since 13 June 2018 and the remediation efforts of 4 July 2018. They were both copied on e-mails and were members of a chat group created to investigate these incidents. The SingHealth CISO was apprised of the investigations but did not make further enquiries. Instead, he waited passively for updates. The SIRM was overseas until 18 June 2018 without nominating a covering officer. During this time, neither the SIRM nor the SingHealth CISO escalated the matter despite their knowledge of these circumstances through meetings and messages. Also, neither the SIRM nor the SingHealth CISO took any steps to activate the SIRT in accordance with the IR-SOP.

31 IHiS senior management and the SingHealth GCIO were only alerted to the attack on the evening of 9 July 2018. Even though the SingHealth GCIO did not receive details of the unauthorised access (and in particular the exfiltration of data), he promptly escalated the matter and informed the CEO of IHiS that there was suspected unauthorised access into the SCM database. Concurrently, the SingHealth GCIO informed the SingHealth

DGCEO (OT&I) of the suspected unauthorised access. After being informed, the CEO of IHiS consulted with IHiS's director for Cyber Security Governance ("CSG") and organised an urgent conference call between IHiS senior management and the relevant employees at 1:00pm the next day, where he was to be briefed on the matter.

32 Details of the attack and the exfiltration of data were first shared with the CEO of IHiS and the SingHealth GCIO, at the conference call on 10 July 2018. The CEO of IHiS immediately recalled all relevant employees and IHiS senior management for an urgent meeting at IHiS's office on the matter and to undertake an examination of IHiS' logs of the attacker's queries on the SCM database to ascertain the extent of data exfiltration (if any). More details of the incident were ascertained and the CEO of IHiS and IHiS senior management were informed of the same at the meeting that afternoon. Arrangements were made to immediately notify CSA. Notifications were also issued by IHiS to MOH and SingHealth. A "war room" with five working cells for containment, investigation, patient impact, communications and reviewing of security measures for other systems was also set up.

Remedial actions

33 From 10 July 2018, IHiS and CSA worked jointly to put in place containment measures to isolate the immediate threat, eliminate the attacker's foothold and prevent the attack from recurring:

(a) IHiS reset the system accounts twice in succession to invalidate any existing full-access authentication tokens that the attacker might have;

(b) IHiS Security Operations Centre was placed on high alert to look out for suspicious activity and signs of compromise and failed login attempts, which allowed CSA and IHiS to detect and respond to fresh callback attempts by the attacker on 19 July 2018 to the C2 servers;

(c) the IHiS Network team tightened firewall rules;

(d) IHiS reloaded all Citrix servers with clean images to ensure no compromised Citrix servers were left running;

(e) IHiS mandated passwords changes for all users (including administrators); and

(f) IHiS put in place extensive monitoring of all administrator accounts.

34 IHiS also supported CSA in its investigations by providing forensic images of computers suspected to be compromised, memory dumps, and proxy and network logs for forensic analysis by CSA. IHiS also simulated the attacker's queries to ascertain the extent of data exfiltration.

35 On 19 July 2018, attempts by the attacker to access the SCM network were again detected and CSA recommended the adoption of Internet Surfing Separation ("ISS") to contain the attack. ISS was instituted immediately thereafter on 20 July 2018 for SingHealth, and by 22 July 2018 for the other two Clusters.

36 Shortly after SingHealth was informed of the cyberattack, SingHealth made plans for patient communications using multiple channels of communication. Within days after the public announcement of the cyberattack on 20 July 2018, SingHealth sent out SMSes or letters to notify patients whether their data was illegally accessed and how they can seek help. Telephone hotlines were also set up for members of the public to obtain further information. Members of the public could also check whether their data had been accessed on the "HealthBuddy" mobile application and the SingHealth website.

37 On 1 November 2018, IHiS announced that it will be adopting a slew of measures to strengthen cybersecurity across the public healthcare sector following the cyberattack. IHiS identified and initiated 18 security measures which will be implemented progressively. Such measures include:

(a) Addressing Advanced Persistent Threat ("APT") by sophisticated actors: IHiS has initiated several measures to improve its ability to detect indicators-of-compromise, record and monitor endpoints' system-level behaviours and events, detect advanced malwares and remove the threats (if any). IHiS will also be implementing two-factor authentication for endpoint local administrators who manage end-user devices and installation of software.

(b) Addressing vulnerabilities to prevent unauthorised access to Clusters' IT networks: To further prevent the use of weak passwords, IHiS will be enhancing the access management capability to manage complex passwords centrally and automatically update and protect administrator accounts. Access

management will be boosted with threat analytics to provide earlier detection of suspicious account activities by applying a combination of statistical modelling, machine learning, as well as behaviour analytics to identify unusual activities, and respond faster to threats.

(c) Enhancing security of the Allscripts SCM: IHiS has put in place database activity monitoring for SCM and it is being enhanced with more comprehensive blocks and alerts on execution of bulk queries.

FINDINGS AND BASIS FOR DETERMINATION

38 The issues for determination are as follows:

(a) whether IHiS was acting as a data intermediary for SingHealth in relation to the SingHealth patients' personal data on the SCM database; and

(b) whether each of the Organisations complied with its obligation under s 24 of the Personal Data Protection Act 2012[5] ("PDPA") in respect of the Data Breach.

39 As a preliminary point, the Commissioner finds that the Patient Particulars and Dispensed Medication Records are personal data as defined under s 2(1) of the PDPA because they contain data about patients who could be identified from that data.

40 Given the facts and circumstances surrounding the Data Breach, the Patient Particulars and Dispensed Medication Records were disclosed without authorisation in the Data Breach.

Whether Integrated Health Information Systems Pte Ltd was acting as a data intermediary for SingHealth

41 A data intermediary is defined in s 2(1) of the PDPA as an organisation that processes personal data on behalf of another organisation but does not include an employee of that organisation. SingHealth engaged IHiS (MOH's designated IT arm of the public healthcare sector), as required by MOH, to manage its IT systems and provide day-to-day

5 Act 26 of 2012.

operations and technical support, maintenance, and monitoring of the entire SingHealth IT system (including the SCM database which held the personal data of SingHealth's patients). These activities include "processing" of personal data on behalf of SingHealth, as defined in s 2(1) of the PDPA.

42 The scope of the IHiS Delivery Group's duties and responsibilities to SingHealth is set out in the following policy documents:

(a) the IT-SPS, which is a policy document jointly prepared by MOHH and IHiS;
(b) the annual IT workplans for each of the SingHealth institutions, which establish an agreement between each of the SingHealth institutions and IHiS;[6] and
(c) the IHiS Data Protection Policy ("DPP") (read in conjunction with the MOHH Information Sharing Policy), which expressly states that IHiS is a data intermediary for SingHealth and all other healthcare institutions in the Clusters.[7]

43 Notably, the DPP makes it clear that IHiS will only collect, use, disclose and/or process SingHealth's data to the extent necessary to fulfil its duties and obligations to SingHealth. This includes, among other things, collecting, using, disclosing and/or processing SingHealth's data for the purposes of investigating and resolution of issues and errors reported in IT programs and systems and IT support.[8]

---

6 The IT workplans expressly include the provision of Sunrise Clinical Manager system maintenance support as an item under the list of "IT System Support and Maintenance Services" to be provided.

7 Clause 1.1.3 of the Integrated Health Information Systems Pte Ltd Data Protection Policy states:

> As IT professionals who support healthcare organisations, *IHIS acts as a 'data intermediary' in relation to Client Data, will exercise reasonable care in protecting Client Data* from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (our '*Protection Obligation*'), and we *undertake steps to ensure that we do not retain personal data longer than is required for business or legal purposes* (our '*Retention Obligation*'). [emphasis added]

8 Clause 6.1.1 of the Integrated Health Information Systems Pte Ltd Data Protection Policy.

44 Pursuant to s 4(2) of the PDPA, a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing has a duty to comply with ss 24 and 25 of the PDPA. Under s 4(3) of the PDPA, an organisation that engages a data intermediary to process personal data on its behalf and for its purposes has the same obligation in respect of such personal data as if it had processed the personal data itself. Accordingly, SingHealth and IHiS each have an obligation to make reasonable security arrangements to protect the personal data of SingHealth's patients that are in their possession or under their control.

The Group Chief Information Officer Office

45 At this juncture, it is pertinent to deal with the issue of where the roles of the GCIO (and the GCIO Office) as well as the CISO fit within the Organisations. Because of the way in which all IT functions and capabilities (including IT staff) for the public healthcare sector are centralised in IHiS, it is not readily apparent whether SingHealth or IHiS is responsible for the actions of the GCIO and CISO.

46 As mentioned at [9] above, every Cluster has a GCIO and CISO. It is not disputed that the SingHealth GCIO and SingHealth GCIO Office are operationally part of SingHealth and its organisational structure. The SingHealth GCIO is positioned at the top of and is in charge of the SingHealth GCIO Office, through which he carries out services and owes responsibilities to SingHealth in terms of overseeing SingHealth's IT systems. In SingHealth, the SingHealth GCIO and his office have a number of duties. These include:

(a) The SingHealth GCIO is responsible for updating the SingHealth Board of Directors on important IT security matters and attends the SingHealth Board IT Committee ("ITC") meetings. For example, the SingHealth GCIO provides SingHealth's Risk Oversight Committee ("ROC") with information relating to proposed or implemented measures to improve SingHealth's IT security, such as encryption of data in SingHealth's servers, monitoring of unusual access to the EMR and outgoing network traffic, and phishing exercises conducted on SingHealth staff. The SingHealth GCIO also informs the ROC about major IT security incidents in SingHealth's

network, remediation of cybersecurity weaknesses observed in SingHealth's servers, and the status of SingHealth's compliance with IT security standards, such as the IT-SPS.

(b) The SingHealth GCIO sits on several SingHealth management-level committees that have oversight over IT matters in SingHealth, specifically the Cluster IT Council ("CITC"), Electronic Medical Record Steering Committee ("EMRSC") and Enterprise Resource Planning Steering Committee ("ERPSC").[9] The SingHealth GCIO Office is also the secretariat of the CITC, the overall governing body for IT matters across the SingHealth Cluster.

(c) The SingHealth GCIO Office oversees SingHealth's IT operations and security and exercises oversight over the IHiS Delivery Group's administration and implementation of policies.

(d) The SingHealth GCIO Office prepares and presents for approval, papers on IT security proposals and budgets, including various annual IT work plans and budgets to SingHealth's management, management committees and board committees, such as the CITC and ITC. The SingHealth GCIO works with the respective SingHealth PHIs to prepare the IT workplan[10] for each SingHealth PHI.

(e) The SingHealth GCIO Office tracks the implementation of audit remediation measures recommended by MOHH's Group Internal Audit division[11] ("GIA") according to the timeline agreed between IHiS and GIA.[12]

---

9 See [66] below for more details on the Cluster IT Council and other board committees in SingHealth with oversight over IT matters.

10 An IT workplan would typically include Integrated Health Information Systems Pte Ltd's direction for implementation of IT initiatives, including IT security initiatives (such as Advanced Threat Protection and hard disk encryption) for the financial year.

11 The scope of the Group Internal Audit division's audits are discussed at [71]–[73] below.

12 The SingHealth Group Chief Information Officer Office does not verify whether the audit remediation measures have been implemented. The Group Internal Audit division would validate if the remediation measures had in fact been performed and update SingHealth management accordingly.

(f) The SingHealth GCIO and GCIO Office also play a key role in SingHealth's staff IT security education and awareness initiatives by developing various security policies pertaining to cybersecurity in accordance with the IT-SPS, such as the SingHealth IT Acceptable Use Policy, the SingHealth Response Plan for Cyber Attacks (Version 3.0) ("SingHealth RP CA"), the standard operating procedure ("SOP") for incident communication and escalation and the SingHealth Data Access Policy. The SingHealth GCIO also sends out memos to all SingHealth staff in relation to IT security risks and staff training initiatives, *eg*, phishing exercises.

47 Similarly, as mentioned at [9] above, it is not disputed that the SingHealth CISO is charged with security oversight for SingHealth and reports to the SingHealth GCIO directly on security matters. The SingHealth CISO does not have any staff reporting under him and relies on the IHiS Delivery Group (specifically the SMD) for its technical expertise on security and operational matters. The SingHealth CISO has a key role in the organisational structure of SingHealth with regard to IT security. Under the IT security incident reporting processes developed and/or adopted by SingHealth, the SingHealth CISO has substantial responsibilities including the assessing, monitoring, and coordinating of responses to such incidents. He is accountable for the actions of incident response functions and is responsible for making regular, direct reports to the SingHealth GCIO, SingHealth management and other relevant parties such as the CSG.

48 On balance, while IHiS employees deployed to fill the SingHealth GCIO or CISO role may owe concurrent duties and responsibilities to IHiS, to the extent that they are carrying out the functions of the SingHealth GCIO or CISO, it is not disputed that they act on behalf of SingHealth. In so far as they perform the work and operate on behalf of SingHealth, the Commissioner finds that the actions of the SingHealth GCIO and CISO as well as the SingHealth GCIO Office should be attributed to SingHealth.

Whether the Organisations complied with their obligations under section 24 of the Personal Data Protection Act

49 Section 24 of the PDPA requires an organisation to protect the 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 (the "Protection Obligation").

50 Pursuant to s 11(1) of the PDPA, the reasonableness of the security arrangements made is to be objectively determined, having regard to what a reasonable person would consider appropriate in the circumstances. The following factors as set out in the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* are taken into consideration in assessing the reasonableness of security arrangements:[13]

(a) the nature of the personal data;
(b) the form in which the personal data has been collected (*eg*, physical or electronic); and
(c) the possible impact on the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

51 In assessing the reasonableness of the security arrangements adopted by the Organisations, the Commissioner took into consideration the fact that medical data is personal data of a sensitive nature which should be accorded a higher standard of protection.[14] The health sector handles some of the most sensitive personal data and patients have the right to expect that the data will be looked after.[15]

52 As observed in *Re The Cellar Door Pte Ltd*[16] ("*Re The Cellar Door*") "reasonable security arrangements" for IT systems must be sufficiently robust and comprehensive to guard against a possible intrusion or attack:[17]

> *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

13 Revised 27 July 2017, at para 17.2.
14 *Re Aviva Ltd* [2019] PDP Digest 145 at [17].
15 UK Information Commissioner's Office, "Health Sector Resources" <https://ico.org.uk/for-organisations/resources-and-support/health-sector-resources/> (accessed 20 April 2019).
16 [2017] PDP Digest 160.
17 *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [29].

> 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.* [emphasis added]

53 The public healthcare sector is heavily reliant on IT and a wide variety of IT systems that hold personal data are employed as part of a healthcare institution's operations.[18] In particular, the SCM system is hosted in H-Cloud and the SCM database contains the full medical records of all SingHealth's patients, which is very sensitive personal information. It is therefore critical to protect the security and confidentiality of such medical records. As highlighted in the *Advisory Guidelines for the Healthcare Sector*:[19]

> In relation to the Protection Obligation, the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control. There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. *Generally, where the personal data stored is regarded as more confidential and where the adverse impact to individuals is significantly greater if such personal data were inadvertently accessed (e.g. relating to sensitive medical conditions), tighter security arrangements should be employed. Healthcare institutions should consider the nature of the personal data in their possession or under their control (as the case may be) to determine the security arrangements that are reasonable and appropriate in the circumstances.* [emphasis added]

Whether SingHealth complied with its Protection Obligation

54 As an organisation subject to the data protection provisions under the PDPA, SingHealth has the primary responsibility of ensuring that there are reasonable security arrangements in place to protect the personal data in its

18 These include clinical systems that provide direct patient care to administrative and infrastructure systems that automate processes and workflow and facilitate sharing of information and communications across teams within and outside of the institution.

19 Revised 28 March 2017, at para 4.2.

possession or under its control,[20] regardless of whether SingHealth has appointed a data intermediary to process patient personal data on its behalf.

55 While SingHealth may outsource the activities necessary to protect the personal data in the SCM database by engaging IHiS to maintain and secure its IT network and the SCM database, SingHealth has a duty to ensure that any data intermediary that processes personal data on its behalf complies with the PDPA.[21] This means that SingHealth can still be liable for a data breach for failing to meet its responsibility, even though IHiS was found to have its own responsibility, and *vice versa*.[22]

56 The Commissioner takes this opportunity to reiterate that while organisations may outsource work to vendors, the responsibility for complying with statutory obligations under the PDPA may not be delegated:[23]

> Further, organisations should take note that while they may delegate work to vendors to comply with the PDPA, *the organisations' responsibility for complying with statutory obligations under the PDPA may not be delegated*. [emphasis added]

57 Having said that, our earlier decisions have recognised that there may be different responsibilities that an organisation or data intermediary may undertake under the PDPA. In *Re Social Metric Pte Ltd*,[24] the Commissioner explained that where the data processing activities are carried out by the organisation's external vendor, the organisation has a *supervisory or general role for the protection of the personal data*, while the data intermediary has a more direct and specific role in the protection of

---

20 Clause 5.1.1 of the Integrated Health Information Systems Pte Ltd Data Protection Policy expressly states that Clients (*ie*, SingHealth) will at all times remain in control over Client Data (*ie*, the personal data of SingHealth's patients).

21 See *Re Smiling Orchid (S) Pte Ltd* [2017] PDP Digest 133 at [46].

22 *Re Social Metric Pte Ltd* [2018] PDP Digest 281 at [16], citing *Re Smiling Orchid (S) Pte Ltd* [2017] PDP Digest 133. See also *Re Singapore Telecommunications Limited* [2018] PDP Digest 148 and *Re Aviva Ltd* [2017] PDP Digest 107.

23 *Re WTS Automotive Services* [2019] PDP Digest 317 at [23].

24 [2018] PDP Digest 281.

personal data arising from its direct possession of or control over the personal data.[25]

58 In this case, on the basis of the Organisations' representations and evidence in these proceedings, the Commissioner is satisfied that SingHealth had some security arrangements in place to meet its supervisory role for the protection of the personal data, such as by maintaining oversight of and control over IHiS' processing of the SCM database. However, the SingHealth CISO's failure to comply with the IT security incident reporting processes and failure to exercise independent judgment call into question whether SingHealth had taken reasonable and appropriate measures to protect the personal data in the SCM database from unauthorised access and copying. More importantly, it points to a larger systemic issue within the organisation.

59 To begin with, parties should put in place a contract that sets out the obligations and responsibilities of a data intermediary to protect the organisation's personal data and the parties' respective roles, obligations and responsibilities to protect the personal data.[26] The foreign data protection authorities have taken the position that a data controller that outsources the processing of its personal data to data processors must take all reasonable steps to protect that information from unauthorised use and disclosure while it is in the hands of the third-party processor.

60 According to the information leaflet on the "Outsourcing the Processing of Personal Data to Data Processors" published by the Hong Kong Office of the Privacy Commissioner for Personal Data's ("PCPD"),[27] the primary means by which a data user may protect personal data entrusted

25 *Re Social Metric Pte Ltd* [2018] PDP Digest 281 at [16], citing *Re Smiling Orchid (S) Pte Ltd* [2017] PDP Digest 133.

26 *Re Singapore Telecommunications Limited* [2018] PDP Digest 148 at [14].

27 Office of the Privacy Commissioner for Personal Data, Hong Kong, "Outsourcing the Processing of Personal Data to Data Processors" (September 2012). Under Hong Kong law, a data user is to take all reasonably practicable steps to safeguard the security of personal data held by it. Where personal data is entrusted to a data processor, a data user is responsible for any act done by the data processor.

to its data processor is through a contract.[28] The PCPD recommends that the following obligations should be imposed on data processors:

> **How to comply with the requirements**
>
> ***Through contractual means***
>
> *The primary means by which a data user may protect personal data entrusted to its data processor is through a contract.* In practice, data users often enter into contracts with their data processors for the purpose of defining the respective rights and obligations of the parties to the service contract. To fulfil the new obligations under DPP2(3) and DPP4(2), data users may incorporate additional contractual clauses in the service contract or enter into a separate contract with the data processors.
>
> The types of obligations to be imposed on data processors by contract may include the following:-
>
> (a) *security measures required to be taken by the data processor to protect the personal data entrusted to it and obligating the data processor to protect the personal data by complying with the data protection principles* (The security measures that are appropriate and necessary for a data user will depend on the circumstances. Basically, the data processor should be required to take the same security measures the data user would have to take if the data user was processing the data himself);
>
> (b) timely return, destruction or deletion of the personal data when it is no longer required for the purpose for which it is entrusted by the data user to the data processor (it is for the parties to agree the appropriate number of days);
>
> (c) *prohibition against any use or disclosure of the personal data by the data processor for a purpose other than the purpose for which the personal data is entrusted to it by the data user*;
>
> (d) absolute prohibition or qualified prohibition (*eg*, unless with the consent of the data users) on the data processor against sub-contracting the service that it is engaged to provide;
>
> (e) where sub-contracting is allowed by the data user, the data processor's agreement with the sub-contractor should impose the same obligations in relation to processing on the sub-contractor as are imposed on the data processor by the data user; where the sub-contractor fails to fulfil

28 However, the Office of the Privacy Commissioner for Personal Data, Hong Kong also recognised that other means of compliance, such as being satisfied that data processors have robust policies and procedures in place and having the right to audit and inspect, may be used.

its obligations, the data processor shall remain fully liable to the data user for the fulfilment of its obligations;

(f) *immediate reporting of any sign of abnormalities* (*eg*, audit trail shows unusual frequent access of the personal data entrusted to the data processor by a staff member at odd hours) *or security breaches by the data processor*;

(g) *measures required to be taken by the data processor (such as having data protection policies and procedures in place and providing adequate training to its relevant staff) to ensure that its relevant staff will carry out the security measures and comply with the obligations under the contract regarding the handling of personal data*;

(h) *data user's right to audit and inspect how the data processor handles and stores personal data*; and

(i) consequences for violation of the contract.

The above list is not exhaustive and data users may need to make adjustments or to include additional obligations on data processors under the contract having regard to factors such as the amount of personal data involved, the sensitivity of the personal data, the nature of the data processing service and the harm that may result from a security breach."

[emphasis added]

61 In a similar vein, the Office of the Privacy Commissioner of Canada's ("OPC") guidance note, "Privacy and Outsourcing for Businesses",[29] states that organisations that outsource the processing of personal information must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times:

> *The Personal Information Protection and Electronic Documents Act* (PIPEDA) — Canada's federal private-sector privacy law – *requires organizations to take privacy consideration into account when considering outsourcing to another organization*.
>
> There is nothing in PIPEDA that prevents organizations from outsourcing the processing of data.
>
> However, regardless of where information is being processed—whether in Canada or in a foreign country—organizations subject to PIPEDA must take all reasonable steps to protect that information from unauthorized uses and disclosures while it is in the hands of the third-party processor.

29 Office of the Privacy Commissioner of Canada, "Privacy Topics – Privacy and Outsourcing for Businesses" (January 2014).

> *Organizations must also be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times.*
>
> [emphasis added]

62 The position taken by the foreign data protection authorities is consistent with the Commissioner's views in *Re Smiling Orchid (S) Pte Ltd*.[30] There should be a clear meeting of minds as to the services the service provider has agreed to undertake and organisations must *follow through with procedures* to check that the outsourced provider is delivering the services:[31]

> Data controllers that engaged 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. [emphasis added]

63 Having reviewed the policy documents at [42] above, the Commissioner finds that IHiS's duties and obligations as a data intermediary are clearly set out and properly documented in the policy documents. In particular:

(a) the IT-SPS sets out IHiS's roles and responsibilities, including design procedures and processes needed to implement the IT security policies and standards as described in the IT-SPS;[32] and

(b) the DPP provides guarantees of security of the personal data processed on behalf of SingHealth as it expressly states that IHiS shall exercise reasonable care in protecting SingHealth's personal data and shall ensure that it implements and maintains

---

30 [2017] PDP Digest 133.

31 *Re Smiling Orchid (S) Pte Ltd* [2017] PDP Digest 133 at [51]. See also *Re Singapore Cricket Association* [2019] PDP Digest 270, where the Commission reiterated that organisations that engage service providers to process personal data on their behalf should clarify and properly document the nature and extent of service provided.

32 Clause 6.1.1 of the Healthcare IT Security Policy and Standards (Version 3.0).

appropriate security measures when processing personal data on behalf of SingHealth.[33]

64 The above policy documents evidence the parties' intentions to be contractually bound by and define the scope of the duties and obligations set out therein.

65 Additionally, SingHealth has developed and implemented a number of data protection policies and practices, which were communicated to its staff. These include:

(a) a Data Protection Policy, which explains how SingHealth institutions handle personal data and is available to the public on SingHealth's website and at its premises;

---

33 Clause 1.1.3 of the Integrated Health Information Systems Pte Ltd ("IHiS") Data Protection Policy:

> As IT professionals who support healthcare organisations, IHIS acts as a 'data intermediary' in relation to Client Data, *will exercise reasonable care in protecting Client Data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (*our *'Protection Obligation')*, and we undertake steps to ensure that we do not retain personal data longer than is required for business or legal purposes (our '*Retention Obligation*'). [emphasis added]

Clause 11.1.1 of the IHiS Data Protection Policy:

> The principles under which we discharge our Protection Obligations as data intermediary under the PDPA for Client Data are as follows:
>
> 11.1.1 When Handling Client Data on behalf of Clients in connection with such services as IHiS may provide to Clients from time to time at Clients' request, *IHiS shall ensure that it implements and maintains appropriate security measures to ensure the security of the Client Data*.
>
> 11.1.2 In doing so, IHiS may be required to appoint vendors to advise on and execute the appropriate data protection measures, and Clients authorise IHiS to appoint such vendors as may be necessary to perform tasks in connection with meeting its obligations under Section 25 *[sic.]* PDPA under its engagement with the Clients.
>
> [emphasis added]

(b) a PDPA Employee Standards Manual, which is a resource and guide for SingHealth employees regarding SingHealth's obligations under the PDPA;
(c) a dedicated Intranet page for PDPA training materials, which is accessible to all staff;
(d) a Master Data Share Agreement that SingHealth entered into with its subsidiary institutions to regulate the sharing of information among the SingHealth institutions;
(e) a Data Access Approval Policy, which sets out the policy and procedure for handling data access requests from data subjects at the SingHealth level; and
(f) a Data Breach Management Policy, which sets out the policy and procedure for the implementation of SingHealth's personal data breach management programme to manage personal data breaches effectively.[34]

SingHealth management and board oversight of IT operations and security

66 Apart from the policy documents, there is evidence that SingHealth maintained oversight of IT operations and security through various oversight and auditing mechanisms, such as through the following board and management committees:

(a) SingHealth's senior management and Board members are apprised of IT matters, such as IT audits and assessments, and the budgeting of IT projects, by the SingHealth GCIO Office;
(b) other than the SingHealth Board of Directors, there are three Board committees that have oversight of IT security matters and meet regularly throughout the year:
    (i) the ITC: a Board committee comprising Board members and co-opted members from external institutions who have IT expertise. Senior management representatives from SingHealth such as the Group CEO ("GCEO") and

34 In the present case, as the suspicious circumstances were first observed by Integrated Health Information Systems Pte Ltd ("IHiS") staff from the IHiS Systems Management Department, the cyber security incident reporting framework which was followed was IHiS's Cluster IT Security Incident Response SOP, version 1.0.

Deputy Group CEO, as well as the SingHealth GCIO attends the ITC meetings. ITC approves the various annual IT workplans for the SingHealth Cluster, which are prepared by the SingHealth GCIO and the IHiS Delivery Group; and

(ii) the Audit Committee ("AC") and the ROC: where audits and key risks relating to cybersecurity matters, such as SingHealth's compliance with and key cybersecurity initiatives undertaken as part of the IT-SPS, and efforts to raise IT user security awareness, are deliberated upon. The ROC receives updates from the SingHealth GCIO on proposed or implemented measures to improve SingHealth's IT security;[35]

(c) at the management level, the CITC is the overall governing body for IT matters across the SingHealth Cluster. The CITC reports to the ITC.[36] The CITC meets monthly to review and endorse SingHealth's Cluster-wide IT projects and initiatives and to oversee and review the IT security program. Its role is to ensure that IT strategy and investments are aligned with the business strategy and IT architecture of the Cluster, resulting in the effective and efficient use of IT in enabling SingHealth to achieve its goals. The SingHealth GCIO sits on the CITC. There are two further sub-committees under the CITC:

(i) the ERPSC; and

(ii) the EMRSC, which is the central governance body to oversee EMR access audit and continuous access monitoring requirements. The EMRSC members include the SingHealth GCIO and the Directors of Medical Informatics of the various PHIs in SingHealth.

---

35 These include updates on the encryption of data in SingHealth's servers, monitoring of unusual access to the EMR and outgoing network traffic, and phishing exercises conducted on SingHealth staff.

36 SingHealth's Group CEO chairs the Cluster IT Council ("CITC") and DGCEO (OT&I) is the Deputy Chair. The CITC members include the other SingHealth DGCEOs and the heads of the various PHIs in SingHealth. The SingHealth GCIO Office is the secretariat of the CITC.

Operational measures

67 In addition to the board and management level oversight, the Commissioner finds that through the SingHealth GCIO and GCIO Office, SingHealth also followed through with operational procedures and checks to ensure that IHiS carried out its functions to protect their personal data.

68 The SingHealth GCIO Office exercises oversight of the IHiS Delivery Group's administration of policies. It monitors and verifies that policies are carried out and issues of security are addressed primarily through various operational meetings between the SingHealth GCIO Office and the IHiS Delivery Group, such as:

(a) the monthly SingHealth IT management, communication and co-ordination meeting chaired by the SingHealth GCIO, where issues of cybersecurity are discussed, allowing the SingHealth GCIO to track and ensure follow up of any outstanding remediation measures to be done;

(b) regular meetings between the SingHealth GCIO Office Application Directors and the individual IHiS Delivery Group teams (*eg*, the SMD), which further allows for cybersecurity issues and policy compliance to be tracked; and

(c) *ad hoc* meetings between the SingHealth GCIO Office and the relevant IHiS Delivery Group teams to track and ensure that detected vulnerabilities in the SingHealth network are addressed.

69 As mentioned at [72] below, the SingHealth CISO also keeps track of the timelines agreed between IHiS and the GIA on the audit remediation measures. In the circumstances, the Commissioner finds that there are governance and audit mechanisms in place for SingHealth to maintain oversight of and control over IHiS's processing of the SCM database.

Audits and risk management

70 The security measures put in place by IHiS are also subject to regular audits. The SingHealth CISO conducts yearly critical information infrastructure ("CII") risk assessments on SingHealth's mission-critical IT systems (*ie*, SingHealth's SCM system) on behalf of SingHealth. This exercise is overseen by the SingHealth GCIO and the SingHealth CISO relies on technical input from members of the IHiS Delivery Group in assessing the risks or threats to the CII, the controls in place and the steps

that should be taken to improve on the existing controls. The SingHealth CISO's assessment is presented to the SingHealth ITC.

71 Separately, MOHH's GIA conducts a CSA CII Compliance Review on the SCM system annually to ascertain if SingHealth, being a CII operator, has complied with CSA's requirements for the CII.

72 The GIA also conducts an annual audit of SingHealth's IT systems.[37] The GIA identifies and prioritises the key risk areas (including for cybersecurity) and comes up with the annual audit plan together with input from SingHealth management for the SingHealth AC's review and approval. The SingHealth CISO coordinates GIA audits by being the parties' point of contact and keeps track of the timeline agreed between IHiS and the GIA on the audit remediation measures.

73 By way of example, in FY 2016, the GIA planned an audit on IHiS' H-Cloud data centre and engaged external providers to perform an IT security penetration test from three PHI systems, one of which was from SGH to H-Cloud (the "H-Cloud Pen-Test"). The plan for the H-Cloud Pen-Test was presented to and approved by the SingHealth AC on 16 May 2016 and the H-Cloud Pen-Test was conducted in early January 2017.

74 As the H-Cloud Pen-Test was an audit of IHiS' H-Cloud, the finalised audit report (the "GIA Audit Report") was addressed to the CEO of IHiS. However, the audit findings (including the security risks) and the follow-up actions and measures to be taken by IHiS were brought to the attention of SingHealth's senior management and were discussed at various board committees and management committees within SingHealth.

75 Between May 2017 and October 2017, the GIA (which was tasked with eventually validating that remediation measures had been carried out) presented the results and observations from the H-Cloud Pen-Test to the

37 The Group Internal Audit division ("GIA") is an independent centralised internal audit division housed within MOH Holdings Pte Ltd ("MOHH") which audits the Clusters and IHiS. Audit findings from the GIA are presented directly to the Audit Committee and the Risk Oversight Committee. Their findings are also addressed by the IHiS Board Audit and Risk Committee. The GIA reports to the MOHH Board Audit and Risk Committee, which comprises all the Audit Committee Chairmen from all the MOHH subsidiaries (including SingHealth and IHiS).

SingHealth Board AC, ROC and ITC and provided updates on the remediation measures and implementation timelines being undertaken by IHiS to rectify the weakness identified in the GIA Audit Report. This shows that SingHealth's various board committees were kept abreast of the follow-up for the remediation measures by the GIA.

76 One area that had previously been identified as a potential issue in the operational monitoring of the remediation of the audit findings was in respect of the implementation by IHiS of firewall rules on the SGH Citrix Servers to block remote desktop protocol traffic from end-user workstations. In its further representations, SingHealth provided evidence that the SingHealth GCIO Office, through the SingHealth CISO, had been tracking the status of the remediation of these outstanding issues. The IHiS Delivery Group had informed the SingHealth CISO on more than one occasion that the implementation of the software firewall rules as a remediation measure had been completed by 7 August 2017. As the implementation of the software firewall rules are a matter of configuration of the existing SGH Citrix Servers without the need for procurement of additional equipment, it is not unreasonable for the SingHealth CISO to have relied on IHiS Delivery Group to provide him with an update after implementation. In retrospect, the SingHealth CISO could have asked for evidence (*eg*, screenshots) demonstrating that the software firewall had been turned on and was effective in blocking remote desktop protocol traffic from end-user workstations. But this would have been a level of operational verification that the SingHealth CISO can reasonably expect the IHiS Delivery Group to have done before it reported to him that this audit finding had been remediated. Having considered SingHealth's further representations, and the evidence provided, the Commissioner accepts that SingHealth had exercised reasonable oversight in respect of the implementation of the software firewall rules.

77 A similar position was taken by the OPC in the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA") Case Summary #2007-365,[38] which relates to the disclosures by the Society for

38 Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2007-365, Responsibility of Canadian Financial Institutions in SWIFT's Disclosure of Personal Information to US Authorities Considered" (2 April 2007).

Worldwide Interbank Financial Telecommunication ("SWIFT") of personal information to US authorities. The OPC reviewed the contract in place between SWIFT and the banks, as well as the other means available to the banks to ensure that SWIFT is providing a comparable level of protection. It found that the banks had fulfilled their obligations under principle 4.1.3 of the PIPEDA, citing the various oversight and auditing mechanisms, such as the development and implementation of a highly sophisticated and elaborate set of security measures, the cooperative oversight and technical oversight group:

> SWIFT and its members have *collaboratively developed and implemented a highly sophisticated and elaborate set of security measures to ensure the integrity, confidentiality, security and reliability* of the financial messages that SWIFT delivers.
>
> *SWIFT reports back to its committees and boards through its Annual Report and through the security audit report* (it should be noted that these reports encompass far more than personal information handling practices).
>
> Although some of the contractual language appears to place SWIFT in control of how its system is used and, by extension, how personal information in its possession is handled, it is nevertheless also obliged to maintain confidentiality of information.
>
> Furthermore, the Assistant Commissioner noted that there are other means by which the banks, as members and users of the SWIFT system, can ensure that a comparable level of protection is in place, particularly with respect to *the cooperative oversight and technical oversight groups. Through these various oversight and auditing mechanisms, and through the contractual language and various security measures in place, she was satisfied that the banks are meeting their obligations under Principle 4.1.3.*
>
> [emphasis added]

SingHealth Cluster Information Security Officer's failure to escalate incident

78 Notwithstanding, as described at [30] above, the Commissioner observes that the SingHealth CISO failed to comply with the various incident response policies and SOPs. The SingHealth CISO's role in relation to cyber incidents are detailed in the following IT security incident reporting policy documents:

(a) under the SingHealth RP CA, the SingHealth CISO's role is to:
  (i) develop and align IT security incident handling and response policies and processes;
  (ii) under the Security Incident Response Plans for various scenarios, *eg*, Malware Infection and Data Loss/Leakage, upon being alerted, the SingHealth CISO is responsible for crucial steps, including:
    (A) to review and classify the incident and notify the relevant personnel, such as the SingHealth GCIO, SingHealth's Corporate Communication Department, the CSG, and the management of affected SingHealth institutions ("Relevant Personnel") within 30 minutes of receiving the alert;
    (B) to prepare the incident report and provide periodic containment and incident closure updates to the Relevant Personnel; and
    (C) for the post-mortem, to finalise and submit the incident report to the Relevant Personnel, and update the SOP for such incidents.

(b) under the IR-SOP, the SingHealth CISO likewise has a direct line of reporting to the SingHealth GCIO and the following responsibilities in a security incident:
  (i) accountable for the actions of the incident response team and incident response functions;
  (ii) responsible for making regular, direct reports to the SingHealth GCIO, the CSG and the management of SingHealth institutions;
  (iii) perform post-incident review of the incident to improve processes;
  (iv) coordinate with SingHealth's Corporate Communication Department;
  (v) where applicable, report to law enforcement authorities; and
  (vi) endorse IT security incident handling and response processes.

79 As mentioned at [47] above, the SingHealth CISO has a key role in the organisational structure of SingHealth with regard to IT security, alongside the SingHealth GCIO. Under the IT security incident reporting

processes developed and/or adopted by SingHealth, the SingHealth CISO has substantial responsibilities including assessing, monitoring, and coordinating responses to such incidents. He is accountable for the actions of the incident response functions and is responsible for making regular, direct reports to the SingHealth GCIO, SingHealth management and other relevant parties such as the CSG.

80 Cybersecurity incidents are investigated by the IHiS SIRT, which is led by the SIRM. As the SingHealth CISO does not have any staff reporting under him, the SingHealth CISO relies on the IHiS Delivery Group for its technical expertise on security and operational matters. Under the IR-SOP, the SIRM is responsible for leading the effort of the SIRT and co-ordinating input from the SIRT members. The SIRM reports to the SingHealth CISO. In turn, the SingHealth CISO is accountable for the actions of the SIRT and is responsible for escalating any issues to the SingHealth GCIO Office.

81 In this case, even though the SingHealth CISO was informed of suspicious activities showing multiple failed attempts to log in to the SCM database using invalid credentials, or accounts that had insufficient privileges in mid-June 2018, and the attack and remediation efforts on 4 July 2018, the SingHealth CISO did not escalate these security events. Rather, he wholly deferred to the SIRM's assessment as to whether an incident was reportable (who operated erroneously under the misapprehension that a cybersecurity incident should only be escalated when it is "confirmed") when he should have exercised independent judgment to escalate the incident to the SingHealth GCIO. To his mind, at the time that he was informed of these suspicious activities, they were only potential breaches and were not confirmed security incidents as investigations were still underway. This does not comply with the IR-SOP. Besides failing to exercise his independent judgment, it would appear that the SingHealth CISO also failed to understand the significance of the information provided to him or to grasp the gravity of the events that were happening.

82 In this respect, the findings of the COI are relevant. Having thoroughly examined the incident response up to 10 July 2018, including the sequence of events and the state of mind of the persons involved, the COI found that with regard to the incidents on 4 July 2018, the SingHealth CISO's response was "clearly lacking, and displayed an

alarming lack of concern".[39] It was clear at that point that a CII system had potentially been breached. The SingHealth CISO should have recognised it as a Category 1 reportable security incident and taken steps to escalate the matter immediately but he did not do so. Instead, he "effectively abdicated to [the SIRM] the responsibility of deciding whether to escalate the incident".[40]

83 Furthermore, although the SingHealth CISO was accountable for the actions of the SIRT under the IR-SOP, the COI found that the SingHealth CISO did not provide any significant degree of leadership in sharing information, co-ordinating investigations and remediation efforts across the various IHiS teams. Instead, the SingHealth CISO "did nothing, and simply left [the SIRM] and the rest of the SIRT to their own devices in the investigation of the matter and remediation efforts".[41]

84 In the circumstances, the Commissioner finds that the SingHealth CISO failed to discharge his duties. For the reasons set out at [47] to [48] above, the SingHealth CISO's failure to comply with the incident reporting SOPs is a lapse that is attributable to SingHealth. While the attacker had already gained access to the SCM network and SCM database by that time, given the substantial volume of sensitive medical personal data held in the SCM database, it is reasonable to expect that someone in the SingHealth CISO's position, with the experience and stipulated responsibilities under the IT security incident reporting processes, should have been more familiar with the incident reporting standards, showed greater initiative and exercised independent judgment to escalate the incident to the SingHealth GCIO. However, the SingHealth CISO's conduct in this case fell far short of what a reasonable person would expect from someone in his position.

85 In its representations, SingHealth referred to evidence of communications between the SingHealth CISO and SIRT personnel between 13 June 2018 and 9 July 2018, which showed that the SingHealth CISO raised queries and sought updates while the SIRT was conducting investigations into the cybersecurity incident. Having reviewed the evidence submitted by SingHealth, the Commissioner finds that the SingHealth CISO had not acted reasonably and failed to discharge his responsibilities.

---

39 Public Committee of Inquiry Report (10 January 2019) at para 514.

40 Public Committee of Inquiry Report (10 January 2019) at para 514.

41 Public Committee of Inquiry Report (10 January 2019) at para 514.

Apart from raising a few questions with regard to the suspicious activities when they first surfaced on 13 June 2018, the SingHealth CISO failed to provide any input or guidance to the team or query whether the matter should be escalated. Rather, the evidence showed that security incidents were handled without sufficient regard for the importance of protecting personal data and discharging its responsibilities properly.

86 SingHealth's representations also drew attention to an important point about the role of the SingHealth CISO from an organisational structure perspective. Because all IT functions and capabilities for the public healthcare sector, including the domain expertise and technical capabilities required to investigate and respond to IT security incidents, are centralised in IHiS, in effect, the SingHealth CISO and GCIO Office have little choice but to rely on the IHiS SMD for their oversight on cybersecurity incidents.

87 The SingHealth GCIO is supported by the GCIO Office, which has a staff strength of about 50 IHiS employees. Together, they are collectively responsible for 11 institutions, with an estimated 30,000 employees, 400-odd IT systems and 350 to 500 IT projects. The SingHealth CISO's responsibilities in the GCIO Office are also relatively broad and include:

(a) working on IT risk assessments;[42]
(b) liaising with the GIA and IHiS Delivery Group for audit confirmation, co-ordinating progress updates and following-up on any audit findings or observations;
(c) being part of the security incident response and reporting process;[43] and

42 The SingHealth Cluster Information Security Officer ("CISO") covers at least four risk assessments (enterprise risks, critical information infrastructure risks, *etc*) each year from the IT perspective. Each assessment would stretch over a few months depending on the complexity of the matter. The SingHealth CISO would also follow up with the Integrated Health Information Systems Pte Ltd Delivery Group to check on the remediation/implementation status.

43 The SingHealth Cluster Information Security Officer ("CISO") would liaise with the Integrated Health Information Systems Pte Ltd ("IHiS") Security Management Department ("SMD") for security event escalation about three to four times a month. In such instances, other IHiS Delivery Group colleagues would inform the SingHealth CISO about potential security issues.

(*continued on next page*)

(d) assisting the SingHealth GCIO in raising end-user awareness of IT security in SingHealth.

88 Given the size and scale of SingHealth's IT systems and network and the large databases of sensitive medical personal data that SingHealth is responsible for, it is reasonable to expect that considerable resources would have been devoted to the SingHealth CISO to carry out operational and security oversight of SingHealth's IT systems. However, the SingHealth CISO (who is the only member of staff who has a portfolio specific to security) worked alone and had no staff reporting under him. As a result of this arrangement, when the SingHealth CISO was on medical leave between 20 June 2018 and 3 July 2018, there was no one other than the IHiS SIRM to cover the SingHealth CISO's duties and provide guidance on the investigation.

89 The SingHealth CISO's failure to discharge his duties is also not a one-off incident that would have been difficult to foresee.[44] Rather, it revealed a systemic problem in the way the SingHealth GCIO Office, specifically the SingHealth CISO function, is staffed. The SingHealth CISO did not have the resources or the technical and IT security expertise for him to properly fulfil his functions. For example, he should have had a team within SingHealth to support him and provide adequate cover when he is away. It was evident from the SingHealth CISO's response to the Data Breach that the existing arrangements are inadequate. As this organisational arrangement failed to meet the reasonable standards expected of an organisation of SingHealth's size, the Commissioner finds that SingHealth had failed to put in place reasonable security arrangements to protect the personal data in its possession or under its control from unauthorised access and copying.

90 In this regard, SingHealth made representations submitting that it relies on and requires IHiS to ensure that the staff they deploy to carry out functions provided by IHiS, such as the SingHealth GCIO and CISO, are appropriately qualified and trained to discharge their duties and do so responsibly. SingHealth has no control over the organisational structure, how the CISO and SIRT are set up, or how the SingHealth CISO has to

---

The SingHealth CISO would liaise with the SMD for follow-up and remediation, and to also obtain confirmation of remediation.

44 See *Re BHG (Singapore) Pte Ltd* [2018] PDP Digest 270 at [25]–[28].

rely on the investigation findings and updates of the SIRT and other teams before making a report upwards or over manpower allocation. It also emphasised that SingHealth shares an atypical relationship with IHiS which goes beyond the typical relationship a vendor shares with a customer – IHiS is not an IT vendor but the MOH-designated IT arm of the public healthcare sector.

91 The Commissioner understands that this is the way the public healthcare sector is structured and is sympathetic to the fact that SingHealth may have had limited ability to influence the organisational structure. Nevertheless, in so far as SingHealth is an organisation as defined in s 2(1) of the PDPA and does not fall within any of the category of organisations that are excluded from data protection obligations under s 4(1) of the PDPA, SingHealth is required to demonstrate that it has complied with the obligations under the PDPA in the event of an investigation.[45]

92 In this regard, as emphasised in earlier decisions and at [54] above, it bears repeating that SingHealth has the *primary role and responsibility* of ensuring the overall protection of the personal data in its possession or under its control, even if it has engaged a data intermediary that has a duty to protect the personal data.[46] The fact that SingHealth is required to engage and rely on IHiS for all its IT services in accordance with MOH's policy does not absolve SingHealth from its responsibilities and obligations under the PDPA. Hence, these representations cannot absolve SingHealth from liability but the Commissioner recognises the exceptional set of circumstances in this case and has taken them into consideration as mitigating factors in the directions that the Commissioner has made.

93 SingHealth also submitted that the errors of individuals within organisations should not in and of itself equate to a breach of s 24 of the PDPA unless the individual's errors point to a larger systemic issue within the organisation or an inadequacy of security arrangements which led to or caused the mistakes, lapses or poor judgment.

---

45 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 6.3.

46 See *Re Management Corporation Strata Title Plan No 3696* [2018] PDP Digest 215 at [16]; *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [33] and [34].

94 The Commissioner agrees that as a matter of principle, an error or flaw in the organisation's systems and processes does not automatically mean that the organisation failed to take reasonable security arrangements to protect personal data. As highlighted in *Re AIG Asia Pacific Insurance Pte Ltd*,[47] the Commissioner will consider whether the organisation had implemented any security arrangements and if so, whether those arrangements are reasonable:

> 27 *The fact that personal data had been disclosed to an unauthorised party by an error or flaw in an organisation's systems and processes does not automatically mean that the organisation is liable under s 24 of the PDPA* for failing to take reasonable security arrangements to protect personal data.
>
> 28 For the purposes of s 24, the *Commissioner has to consider what security arrangements (if any) an organisation had implemented to prevent such unauthorised disclosure, and whether those arrangements are reasonable*.
>
> [emphasis added]

95 In the present case, as the Commissioner has found at [87] to [89] above that the SingHealth CISO's failure to comply with the SOPs was emblematic of the inadequacy of the security arrangements, the Commissioner has already taken this into consideration before SingHealth submitted its representation.

96 Having carefully considered all the relevant facts and representations made by SingHealth, the Commissioner finds that while SingHealth had maintained oversight of IHiS' provision of IT operations and security through various levels of board, management and operational oversight and audit mechanisms, SingHealth had not taken sufficient security measures to protect the personal data in the SCM database from the unauthorised access and illegal copying. Accordingly, SingHealth has failed to meet its Protection Obligation and is in breach of s 24 of the PDPA.

Whether Integrated Health Information Systems Pte Ltd complied with its Protection Obligation

97 At the outset, as the personal data in the SCM database was in IHiS's possession, if not under its control, IHiS was obliged to implement

47 [2019] PDP Digest 189 at [27] and [28].

reasonable security arrangements to protect the personal data in the SCM database.

98 It is accepted that the Data Breach was perpetrated by a skilled and sophisticated threat actor. The level of discipline and planning demonstrated during the Data Breach are characteristic of an APT actor, who used advanced methods that overcame enterprise security measures:

(a) the attacker took steps to conduct lateral movement and reconnaissance in order to avoid breaching the existing detection mechanisms IHiS had put in place, and could not have easily been noticed;
(b) the attacker used highly customised malware that evaded SingHealth's anti-virus software and security defences and could not have been detected by standard anti-malware solutions; and
(c) the attacker employed numerous customised and modified open-source scripts and tools that were manipulated to evade signature-based anti-virus detection.

99 Furthermore, the attacker deliberately and specifically targeted the SCM database and took active steps to ensure that it would remain undetected until it had reached the SCM database.

100 Hence, the key issue for determination is whether, despite the attacker's sophisticated and novel tactics, techniques and procedures, IHiS had done enough under s 24 of the PDPA to prevent the unauthorised disclosure.

Integrated Health Information Systems Pte Ltd's security arrangements at the material time

101 IHiS bases its security arrangements on the IT-SPS,[48] which is a policy based on international information security standards. The IT-SPS covers all the essential IT security domains, and prescribes the IT security policies, technical security standards and processes to be implemented by all public healthcare institutions, including policies on user access control and password management.

48 The current version of the Healthcare IT Security Policy and Standards (Version 3.0) was issued in 2014.

102 According to IHiS, it maintained a comprehensive IT security incident and response framework, which consists of three measures – prevention, detection and response, for all systems under its purview (including the SCM network during the time of the Data Breach). A brief summary of the measures taken for the SCM network is as follows:

(a) technical measures to prevent cybersecurity risks for:
    (i) end-point security relating to SingHealth and IHiS issued end-point devices (*eg*, workstations), such as the prohibition of use of personal devices on the SCM network, the use of anti-virus and anti-malware software;
    (ii) network security, such as creating network firewalls to segregate each network segment so as to ensure that only authorised network traffic is permitted to cross segments or zones;
    (iii) H-Cloud security by implementing measures such as web application firewalls, physical separation of virtual data centres, and privileged access management;
    (iv) database security, such as by running automated scripts which closely monitor the SCM database to detect and raise alerts for performance abnormalities, and keeping detailed access and audit logs which include information such as failed login attempts; and
    (v) e-mail security, such as anti-virus, anti-spam and attachment blocking technology;
(b) policies and processes to manage or otherwise deal with cybersecurity risks, which include:
    (i) building awareness and educating staff on cybersecurity risks and IHiS' IT policies, such as by conducting IT security training, sending regular security alerts and conducting regular phishing exercises to create awareness and promote vigilance;
    (ii) developing policies for users, such as the IT-SPS, the SingHealth Acceptable Use Policy, and the SingHealth End User Computing, Equipment and Network Policy and monitoring the compliance of users to these policies; and
    (iii) conducting periodic reviews of the risks, controls and other measures of the security systems flagged by the GIA;

(c) detection measures to identify and pinpoint cybersecurity risks, such as continuous real-time monitoring and periodic testing; and

(d) risk assessment exercises carried out at various levels. For example, enterprise risk assessment and CII risk assessment exercises were conducted annually by the SingHealth CISO and overseen by the SingHealth GCIO.

103 At the material time, IHiS also had the following incident reporting processes and frameworks in place to ensure that cybersecurity incidents are appropriately escalated and addressed:

(a) the SIRF, which translates the requirements of the National Cyber Incident Response Framework[49] into the context of the PHIs; and

(b) the IR-SOP, which is IHiS' Cluster-level standard operating procedure for responding to security incidents.

104 Internally, IHiS also maintains a security incident classification framework identical to that used by CSA and has developed internal reporting timelines for security incidents to be escalated to the CSG within IHiS.

105 Cybersecurity incidents are investigated by the IHiS SIRT. This team is led by the SIRM and comprises IHiS' Computer Emergency Response Team ("CERT") and lead personnel from IHiS Infrastructure Services and Application Services teams. It is the SIRM's responsibility to co-ordinate input from the SIRT members and to report to the SingHealth CISO. The SingHealth CISO's responsibility is to escalate any issues to the SingHealth GCIO.

106 As mentioned at [127] below, IHiS represented that all IHiS staff have been briefed to alert the SIRT or the SMD when a non-security IHiS member of staff encounters a suspicious incident. This was communicated to all IHiS staff through regular e-mails, circulars, wallpapers and intranet banners. IHiS also represented that in so far as the non-security IHiS staff are concerned, the general expectation was for them to report suspicious

49 The National Cyber Incident Response Framework is the framework for the reporting and management of cyber incidents affecting critical information infrastructures.

incidents to the SIRT or SMD. Such staff are not expected to be familiar with the details of the IT-SPS and SIRF, though these policies were made available via IHiS' Intranet.

107 Given that IHiS regularly handles large volumes of sensitive personal data on behalf of the PHIs, the Commissioner finds that it is insufficient for IHiS to have merely informed its non-security staff to alert the relevant personnel through e-mails, circulars, wallpapers and Intranet banners. These are effective in creating awareness amongst staff, but ineffective as policies for a number of reasons. E-mails and circulars are disseminated and therefore ineffective as a resource for future reference; while wallpapers and Intranet banners are temporary and replaced eventually. The necessity of a set of written policies that are centrally stored (*eg*, on the Intranet) and which can be consulted cannot be replaced by these other means of creating awareness. IHiS had admitted that while the SIRF and IT-SPS were made available via IHiS's Intranet, it had not developed any written policy on IT security incident reporting for its non-security staff. Furthermore, regular training sessions and staff exercises should have been conducted to ensure that all IHiS staff are familiar with the IT security incident reporting and their role in recognising and reporting suspected IT security incidents. These trio of awareness, training and written resource have to be deployed collectively for an effective staff training programme.

108 As the Commissioner observed in *Re SLF Green Maid Agency*,[50] it is insufficient for organisations that handle large volumes of sensitive personal data to merely disseminate guidelines and instructions. It is necessary for the organisation to have a system of staff training and awareness:

> For a company like the Organisation that handles personal data of foreign domestic workers and clients on a daily basis (*eg*, passport and income information), it is *necessary for it to put in place a better system of staff training and awareness given the sensitive nature of personal data that it handles, as well as the volume. Merely disseminating guidelines and verbal instructions is insufficient*. As noted in *Re Aviva Ltd*, whilst there is no specific distinction in the PDPA based on the sensitivity of the data, organisations are to ensure that there are appropriate levels of security for data of varying levels of sensitivity. NRIC and passport numbers and financial information would generally be considered more sensitive. *Structured and periodic training could have been implemented to protect personal data.* [emphasis added]

50 [2019] PDP Digest 327 at [13].

109 Furthermore, the Commissioner finds that by IHiS's own admission, there were a number of vulnerabilities and gaps in SingHealth's network and in IHiS's systems and processes which were exploited by the attacker.

110 First, there were gaps in how IHiS's policies and practices were implemented and enforced, particularly in the management of the SGH Citrix Servers. IHiS asserts that its management gave clear directions and instructions to its Citrix Team Lead in July 2017 to turn on software firewall on the SGH Citrix Servers to block remote desktop protocol traffic from end-user workstations. However, firewall rules were not implemented on the SGH Citrix Servers that were used by the attacker in the course of the attack. IHiS's staff failed to discharge their assigned responsibilities. IHiS had relied on its staff to follow through on instructions and the Citrix Team Lead to ensure that the instructions were complied with. In this case, however, both the team responsible for placing the firewalls and their supervisor, the Citrix Team Lead, failed to discharge their assigned responsibilities. To compound matters, IHiS updated the SingHealth CISO that the software firewall rules had been implemented without having verified this.

111 Second, there were insufficient steps taken to ensure that technical measures to protect personal data were carried out as intended and according to IHiS's own policies and practices. Such insufficiencies were exploited by the attacker.

112 *Weak local administrator passwords*: under the IT-SPS, administrator accounts were required to have a 15-character password. Notwithstanding, the local administrator account that the attacker relied on in the course of the attack had an easily deduced password ("P@ssw0rd") with only eight characters. The account also had the same password since 2012 despite the requirement for it to be changed every three to six months. Although IHiS had pushed its password policy and requirements through a Group Policy Object ("GPO"), which should apply to all servers by default, it did not apply to servers which had activated a setting to prevent the GPO from applying, such as the SGH Citrix Servers.[51]

---

51 Group Policy Objects ("GPOs") automate the implementation and enforcement of policies. They should apply to all servers by default, except for groups of servers which have the "block policy inheritance" setting applied. Applying "block policy inheritance" prevents group policies from being

(*continued on next page*)

113 In *Re Orchard Turn Developments Pte Ltd*,[52] the Commissioner highlighted (at [35]) the importance of managing admin account credentials, and took the view that the implementation of an effective password expiry mechanism would have reduced the potential adverse impact of an unauthorised use of the admin account password:

> 35 On the facts, the *Organisation failed to put in place any formal policy or practice for the management of the admin account passwords to the EDM server*. Additionally, in terms of the Organisation's handling of the admin account credentials, the Commission identified two main areas of concern as follows:
>
> …
>
> (b) second, *the password of the admin account to access the EDM Application had not been changed since the roll out of the EDM Application*, i.e. from November 2014 until the time of the data breach incident in December 2015. *The implementation of an effective password expiry mechanism would have reduced the potential adverse impact of an unauthorised use of the admin account password.*
>
> [emphasis added]

114 *Passwords in cleartext was found in scripts*: the password of one of the local administrator accounts relied by the attacker in the course of the attack was found in cleartext in scripts on an SGH Citrix Server. This script was created by a Citrix Administrator despite specific instructions in March 2017 and June 2017 from his supervisors to clean up the scripts and avoid storing any passwords in the scripts in cleartext. Under the IT-SPS, passwords must not be stored as cleartext on storage systems, audit logs or when transmitted over the network but should configured to be encrypted, prompted or hashed.

115 In *Re The Cellar Door*, the fact that login credentials were being transferred in clear and unencrypted text, which exposed the hosting environment to potential compromise should the credentials be intercepted,

---

inherited from these servers. The SGH Citrix Servers were part of a group of servers which had group policy inheritance applied. As such, the GPOs implementing the complex password policy and policy for the deactivating of dormant accounts were not applied.

52 [2018] PDP Digest 223.

was found to be indicative of a poor level of security in the system design and implementation:[53]

> In this case, the Respondents have failed to put such an all-round security in place. *The Commission has found several significant gaps in the security measures implemented as follow*:
>
> …
>
> (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 in the necessary measures to secure the transmission of the login credentials.
>
> [emphasis added]

116 *Dormant accounts were not disabled*: although IHiS's policies required a periodic review of unused or dormant accounts, the dormant local administrator account and service account relied on by the attacker in the course of the attack were not detected and disabled by IHiS because the automated process to detect and disable unused or dormant accounts only extended to "domain" accounts instead of local accounts.[54]

---

53 *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [30].

54 Domain accounts exist in the Microsoft Active Directory and are used to centrally manage servers and workstations within an enterprise when these computing resources join to a domain. In contrast, local accounts exist within each server or workstation and are not managed centrally.

117 In *Re K Box Entertainment Group Pte Ltd*,[55] the Commissioner found (at [26]) that the organisation had weak control over unused accounts. The organisation failed to make reasonable security arrangements to protect the personal data in its possession or under its control as it could have easily removed the unused accounts, but it had failed to do so. As a result, the unused administrative account with a weak password ("admin") remained in the system and put the personal data of the organisation's members at risk:

> 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:
>
> …
>
> (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 system 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 system, 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;
>
> …
>
> [emphasis added]

55 [2017] PDP Digest 1.

118 *Lack of controls to detect bulk querying behaviour in the SCM database or queries being run from illegitimate client applications*: even though the SCM database contained sensitive personal data of millions of patients, there were no controls to detect bulk querying behaviour. However, IHiS represented that the use of such database access monitoring software or tools are not common in the healthcare sector and are generally only used in the security and banking/finance sector. The Public COI Report corroborates this.[56] As such, the Commissioner accepts that it was not unreasonable that IHiS did not have such controls in place at the material time.

119 That said, according to the Guide to Securing Personal Information issued by the Office of the Australian Information Commissioner ("OAIC"),[57] the use of proactive monitoring to identify possible unauthorised access or disclosure may be a reasonable step to take particularly if the organisation uses many systems or databases which hold large amounts of personal information:

> **Audit logs, audit trails and monitoring access**
>
> Unauthorised access of personal information can be detected by reviewing a record of system activities, such as an audit log. Maintaining a chronological record of system activities (by both internal and external users) is often the best way for reviewing activity on a computer system to detect and investigate privacy incidents. Audit logs should also be named using a clear naming convention.
>
> Audit trails are used to reconstruct and examine a sequence of activities on a system that lead to a specific event, such as a privacy incident.
>
> *Access monitoring software that provides real time (or close to real time) dynamic review of access activity can also be useful for detecting unauthorised access to personal information. Use of proactive monitoring to identify possible unauthorised access or disclosure*, including any breach that might amount to an eligible data breach for the purposes of the NDB scheme, *may be a reasonable step for you to take particularly if you use many systems or databases which hold large amounts of personal information*.
>
> [emphasis added]

56 Public Committee of Inquiry Report (10 January 2019) at para 221.

57 Office of the Australian Information Commissioner, "Guide to securing personal information: 'Reasonable steps' to protect personal information" (June 2018) <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information> (accessed 20 April 2019).

120 In future, organisations that hold large amounts of personal data should consider implementation of database access monitoring as one of the security measures for early detection of unauthorised access or disclosure.

121 *Lack of controls to prevent or monitor communications between the SGH Citrix Servers and the SCM database at HDC*: such controls were only implemented after the unauthorised access from the SGH Citrix Servers to the SCM database was discovered. Even if it was necessary to keep a connection between the SGH Citrix Servers and the SCM database at HDC, such a connection should have been a protected connection and the servers using the connection should have been placed behind a firewall (which they were not).[58]

122 As highlighted in *Re The Cellar Door*, *a* firewall is a fundamental measure that should be in place for servers to protect against an array of external cyber threats:[59]

> In this case, the Respondents have failed to put such an 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.*
>
> [emphasis added]

123 *Unpatched Microsoft Outlook e-mail client maintained in the SingHealth IT environment*: the attacker was able to gain access to an unpatched end-user workstation running a version of Outlook by using a publicly available hacking tool. On this issue, IHiS submitted that it did not assess if an urgent roll-out to deploy the patch outside its usual patching cycle was required given that the patches released by Microsoft were not categorised as "critical". In the circumstances, the Commissioner accepts that it was not unreasonable for IHiS to not have applied the patch at the

58 As found at [110] above.

59 *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [30].

material time. IHiS cannot be faulted for relying on the software provider's assessment of the criticality and urgency for applying the steady stream of updates and patches that are made available on a regular basis.

124 Notwithstanding, the Commissioner takes this opportunity to reiterate the importance of putting in place maintenance processes to ensure regular security patching as a security measure. Patching is one of the common tasks that all system owners are required to perform in order to keep their security measures current against external threats:[60]

> First, *the Organisation failed to ensure regular patching of the EDM Application since its roll out* in November 2014. The KPMG Reports highlighted that the EDM Application was exposed to 24 known vulnerabilities because it did not follow a regular patching cycle. The KPMG also noted that the *EDM server appeared to have been patched in an* ad hoc *manner once every two to four months. Patching is one of the common tasks that all system owners have to perform in order to keep their security measures current against external threats. The failure to patch the EDM Application regularly was a failure to protect the EDM Application against known system vulnerabilities.* [emphasis added]

125 For completeness, even though the SingHealth GCIO had oversight of the IHiS Delivery Group's administration and implementation of policies, seeing as the above vulnerabilities are basic operational tasks that fall within the type of day-to-day operations and technical support, maintenance and monitoring, which is managed by the IHiS Delivery Group, it was reasonable for SingHealth to have expected the IHiS Delivery Group to ensure that reasonable security arrangements which were within the scope of IHiS's responsibility were carried out.

126 Third, vulnerabilities that had previously been flagged to IHiS were either not remediated or not addressed in time:

(a) IHiS was aware of some vulnerabilities in the Citrix Servers and had required its Citrix Team to fix the Citrix Servers to prevent exploitation. Although the Citrix Servers in H-Cloud were fixed, the same fixes were not applied to the SGH Citrix Servers, some of which were still in operation even though they were planned to be decommissioned.

---

60 *Re Orchard Turn Developments Pte Ltd* [2018] PDP Digest 223 at [38]. See also *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [26].

(b) The GIA Audit Report had flagged most of the vulnerabilities highlighted in [110] to [123] above. Although IHiS had instructed its staff to address the vulnerabilities stated in the report, IHiS staff responsible for the remediation did not adequately track and ensure that all vulnerabilities were fully and properly remediated. Remediation was stated to be done when it was not actually done or not done thoroughly. No verification was conducted by IHiS line management. In particular, there was evidence that both IHiS and the GIA thought the implementation of firewall rules on the SGH Citrix Servers to block remote desktop protocol traffic from end-user workstations as a remediation measure had been completed by 7 August 2017[61] even though the team responsible for placing the firewall failed to discharge their assigned responsibilities (as observed at [110] above).

(c) A coding vulnerability in the SCM application was flagged by a former IHiS employee in 2014 in an e-mail sent to a competitor of Allscripts. Although the fact that there was a potential vulnerability in the SCM application was known to the management at IHiS at the time, no action was taken to investigate or remedy the vulnerability that he found. IHiS submitted that no action was taken at the time because it took the view that the vulnerability was not an issue, especially in the light of its existing security measures and doubts over the credibility of its former employee. Allscripts had also been alerted to the possibility of a vulnerability. Pertinently, the SCM application is Allscripts's product. Allscripts did not inform IHiS of this apparent coding vulnerability and if this vulnerability will be remediated. It was not unreasonable for IHiS to assume that Allscripts would have issued a patch as part of its regular software support had they verified this apparent coding

61 At the SingHealth Audit Committee meeting held on 13 October 2017, the Group Internal Audit division, which was in charge of ensuring that remediation measures were implemented and checked upon, stated that the implementation status of past audit issues was largely on track. According to the Integrated Health Information Systems Pte Ltd Delivery Group, the specific remediation measure of network segregation enhancement had already been completed.

> vulnerability. In view of this and the fact that the attacker could have used a different method to exploit the coding vulnerability in the SCM client application (that was likely also unknown to Allscripts at the time), which allowed the attacker to retrieve the SCM database login credentials from the H-Cloud Citrix Server, the Commissioner accepts that it was not unreasonable for IHiS to not have remedied the apparent coding vulnerability in the SCM application highlighted in 2014.

127 Fourth, even though IHiS represented that it had communicated to all IHiS non-security staff through regular e-mails, circulars, wallpapers and Intranet banners that the SIRT or SMD should be alerted whenever they encounter a suspicious incident, the fact that IHiS employees who first encountered the suspicious activity failed to escalate it to the SIRT, as opposed to notifying an individual who happened to be part of the SIRT, suggests that the approach adopted by IHiS (where there was no written IT security incident policy in place and no training) was inadequate and IHiS non-security staff did not have a good understanding of the importance and requirements for reporting IT security incidents. The SIRM also failed to comply with the SIRF and IR-SOP.[62]

128 In January 2018, when the SIRM was alerted to callbacks to a suspicious foreign IP address from the workstations compromised by the attacker, he did not take steps to block that IP address for the entire SCM network, or initiate any investigations, which could have identified and contained the compromised workstations before they were eventually used in the attack, including a compromised workstation which was eventually used as a means of exfiltration ("January 2018 incident"). The SIRM failed to escalate the January 2018 incident as he took the position (which IHiS did not endorse) that this was not a reportable incident as it pertained to a malware infection that had been detected and cleaned without network

62 In this regard, the Public Committee of Inquiry Report (10 January 2019) also highlighted (at paras 926 and 927) that even within the Integrated Health Information Systems Pte Ltd ("IHiS") Security Management Department, the processes for reporting observations were inconsistent and unclear. There was no established procedure for how IHiS staff should escalate a matter internally or how to report a security incident to the SingHealth Cluster Information Security Officer or the SingHealth Group Chief Information Officer. This resulted in confusion and consequent delays in response.

propagation. In fact, the SIRM did not make any effort to determine whether there had been any such network propagation.

129 From mid-June 2018, when IHiS staff had identified multiple failed login attempts to the SCM database originating from the compromised SGH Citrix Servers, using invalid credentials, or accounts that had insufficient privileges, the SIRM failed to escalate or take any additional steps to manage the vulnerabilities, as he was labouring under the misapprehension that a cybersecurity incident should only be escalated when it is "confirmed". The SIRM failed to appreciate that timely incident reporting, in accordance with the relevant IHiS policies and standards on incident reporting, could enable more resources to be deployed to better investigate and contain a cybersecurity incident.[63]

130 As highlighted in *Re National University of Singapore*,[64] data protection policies and practices are only effective when staff understand and are familiar with the policy and put its security procedures in practice:[65]

> 24 … In another case, the Office of the Privacy Commissioner of Canada ("OPC") explained that whilst security policies and procedures are essential, they are not in themselves sufficient to protect personal information; *the effectiveness of security safeguards depends on the organisation's*:
>
> > *… [d]iligent and consistent execution of security policies and procedures [which] depends to a large extent on ongoing privacy training of staff and management, so as to foster and maintain a high organizational awareness of informational security concerns.*
>
> 25 In a separate investigation, the OPC further clarified its position and stated that security policies and practices are only effective when '*properly and consistently implemented and followed by employees*'.
>
> [emphasis added]

63 The Committee of Inquiry also found at ([433] and [593]) that he had delayed reporting because he felt that additional pressure would be put on him and his team once the situation became known to management. The evidence also suggested that the reluctance to escalate potential security incidents may have come from a belief that it would not reflect well in the eyes of the organisation if the matter turned out to be a false alarm.

64 [2018] PDP Digest 155.

65 *Re National University of Singapore* [2018] PDP Digest 155 at [24] and [25].

131 However, it was apparent from the response of a number of IHiS staff and in particular, the SIRM's response, that the communications and training provided to them was inadequate for them to fully comprehend and internalise the existing framework and SOPs.

132 To be clear, the PDPA does not require an organisation to provide an *absolute guarantee* for the protection of the personal data in its possession or under its control. As the Commissioner clarified in *Re Tiger Airways Singapore Pte Ltd*:[66]

> In the context of s 24, this means that *an organisation is not required to provide an absolute guarantee for the protection of personal data in its possession, but that it must make such security arrangements as a reasonable person would consider appropriate, given the nature of the personal data involved and the particular circumstances of that organisation*. [emphasis added]

133 Even so, in consideration of the facts and circumstances surrounding the Data Breach, the Commissioner finds that IHiS had not done what a reasonable person would consider appropriate to prevent the unauthorised exfiltration of the personal data in the SCM database. In view of the very large volume of sensitive medical personal data managed and processed by IHiS on behalf of SingHealth, it is reasonable to expect IHiS to accord SingHealth's IT systems and, in particular, the SCM database a higher standard of protection. However, by IHiS's own admission, the weaknesses, lapses and failures on the part of some IHiS personnel to comply with IHiS's security framework showed that the administrative or organisational security measures that IHiS had in place at the time of the Data Breach were inadequate.

134 Accordingly, even though IHiS had in place a number of security arrangements to protect the personal data in its possession or under its control, the Commissioner finds that IHiS had not taken sufficient security steps or arrangements to protect the personal data in the SCM database from unauthorised access, collection, use, disclosure and copying.

---

66 [2018] PDP Digest 166 at [17]. See also *Re BHG (Singapore) Pte Ltd* [2018] PDP Digest 270 at [25].

DIRECTIONS

135 Having considered the evidence obtained by the Commission during its investigation and the representations of the parties, the Commissioner is satisfied that both SingHealth and IHiS have breached s 24 of the PDPA. The Commissioner is empowered under s 29 of the PDPA to give such directions as he deems fit to ensure compliance with the PDPA.

136 The Commissioner hereby directs SingHealth to pay a financial penalty of $250,000 within 30 days of the issuance of this direction, failing which interest at the rate specified in the Rules of Court[67] in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

137 The Commissioner hereby directs IHiS to pay a financial penalty of $750,000 within 30 days of the issuance of this direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

138 The financial penalties imposed against the two Organisations are individually the highest and second-highest financial penalty amounts imposed by the Commission to date. This is appropriate given the circumstances.

139 First, this is the largest data breach suffered by any organisation in Singapore with the number of affected individuals amounting to almost 1.5 million unique individuals. Second, while the attacker managed to exfiltrate the personal data of almost 1.5 million unique individuals, the SCM database which was attacked contained patient data belonging to over 5.01 million unique individuals whose personal data was put at risk. This increases the seriousness of IHiS and SingHealth's data security inadequacies. The patient data held in the SCM database contained highly sensitive and confidential personal data including clinical episode information, clinical documentation, patient diagnosis and health issues and Dispensed Medication Records. It is not difficult to imagine the potential embarrassment that a patient may suffer if such sensitive information about the patient and the patient's health concerns were made known to all and sundry. As such, it is critical for the Organisations to

67 Cap 322, R 5, 2014 Rev Ed.

protect the security and confidentiality of such medical records. Third, the attacker exfiltrated the Dispensed Medication Records of 159,000 unique individuals together with the Patient Particulars. From the Dispensed Medication Records, one may be able to deduce the condition for which a patient was being treated. This may include serious or socially embarrassing illnesses.

SingHealth's representations

140 SingHealth made representations for a reduction in the quantum of the financial penalty as set out in the preliminary decision on the basis that the Commission should factor in the principle of proportionality in deciding the appropriate financial quantum and the extent to which SingHealth had failed to discharge its obligations. In this regard, SingHealth represented that it did have in place various security measures which were reasonable to have oversight of its data intermediary except in relation to the lapses of an individual.

141 The fact that an organisation has adequately implemented other protection policies will not operate to absolve or mitigate liability for breaches. In *Re Funding Societies Pte Ltd*,[68] the organisation pleaded in mitigation that it had in place "a framework of security arrangements, such as a risk management framework, an information security policy and training and audits of its policies and procedures." In response, the Commissioner stated:[69]

> Neither should *the fact that the Organisation continuously assessed its compliance with the obligations set out in the PDPA and that it had the necessary frameworks in place mitigatory as these were the standard of conduct expected for compliance*. These are not activities or measures which go beyond the standard of protection required by the PDPA and as such are not mitigating factors. [emphasis added]

142 Even in cases where both the organisation and data intermediary have been found to be in breach of the PDPA, the Commissioner will assess each party's breach on its own merits and circumstances. In calculating the quantum of the financial penalty to be imposed, the Commissioner takes an

68 [2019] PDP Digest 341.

69 *Re Funding Societies Pte Ltd* [2019] PDP Digest 341 at [32] and [33].

objective approach in assessing the facts and circumstances of the contravention and how a reasonable organisation or data intermediary should have behaved in the circumstances. In this regard, as explained in the *Advisory Guidelines on Enforcement of the Data Protection Provisions*,[70] one of the factors that the Commission may consider to be an aggravating factor includes:

> [T]he organisation is *in the business of handling 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), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure* of that personal data. [emphasis added]

143 Nevertheless, in assessing the breach and determining the directions to be imposed on SingHealth, the Commissioner took into account the following mitigating factors:

(a) SingHealth voluntarily and unequivocally admitted to the facts, accepted the Commission's findings set out in this decision and had agreed to co-operate with the Commission to expedite the Investigation and the determination of liability for each of the parties and issue any directions that the Commission deems fit;

(b) SingHealth was constrained, in that, as a matter of policy, all IT functions and capabilities for the public healthcare sector (including the proposed structure and resourcing for the SingHealth GCIO Office) are centralised in IHiS;

(c) SingHealth was co-operative during the Investigation;

(d) SingHealth took immediate effective remedial action following the Data Breach; and

(e) SingHealth was as much a victim of the malicious actions of a skilled and sophisticated threat actor who used advanced methods that overcame enterprise security measures as the individuals whose personal data was illegally accessed and copied.

144 Similarly, in assessing the breach and determining the directions to be imposed on IHiS, the Commissioner took into account the following mitigating factors:

---

70 21 April 2016, at para 25.2.5.

(a) IHiS voluntarily and unequivocally admitted to liability and had agreed to co-operate with the Commission to expedite the Investigation and the determination of liability for each of the parties and issue any directions that the Commission deems fit;
(b) IHiS was co-operative during the Investigation;
(c) IHiS took immediate effective remedial action following the Data Breach; and
(d) IHiS was as much a victim of the malicious actions of a skilled and sophisticated threat actor who used advanced methods that overcame enterprise security measures as the individuals whose personal data was illegally accessed and copied.

145 Without the above mitigating factors, the Commissioner would have imposed the maximum financial penalty allowed under the PDPA against IHiS and a financial penalty at a significantly higher quantum against SingHealth.

146 The Commissioner has not set out any further directions for IHiS and SingHealth given the remediation measures already put in place.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re COURTS (Singapore) Pte Ltd

[2019] PDP Digest 432

Coram: Tan Kiat How, Commissioner
Case Number: DP-1707-B0917
Decision Citation: [2019] PDP Digest 432; [2019] SGPDPC 4

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

22 January 2019

BACKGROUND

1 On 9 July 2017, the Personal Data Protection Commission (the "Commission") received a complaint from a customer ("Complainant") of COURTS (Singapore) Pte Ltd ("COURTS") stating that the http://www.courts.com.sg website ("Website") was "*unsafe for customers*". The Complainant discovered that by entering his name and e-mail address on COURTS' Guest Login ("Guest Login Page") for the purpose of making a purchase, the Website would automatically open another webpage ("Guest Checkout Page") disclosing the Complainant's contact number and address (the "Incident").

2 Following an investigation into the matter, the Commissioner found COURTS in breach of s 24 of the Personal Data Protection Act 2012[1] ("PDPA").

MATERIAL FACTS

3 The Website is owned and managed by COURTS, a leading consumer electronics and furniture retailer in Singapore with a network of 80 stores nationwide. Ebee Global Solutions Pvt Ltd ("Ebee") was an IT

1 Act 26 of 2012.

vendor engaged by COURTS to develop and maintain the Guest Login Page and Guest Checkout Page ("Guest Checkout System") that was part of the Website. At the material time, the process flow when a customer wished to make a purchase through the Guest Login Page was as follows:

(a) the customer accesses the Website and selects an item to "Add to cart" before selecting "Proceed to checkout";
(b) the customer may choose to log into his COURTS' HomeClub account or he may choose to "Checkout as guest user";
(c) if the customer chooses to check out as a guest user, he enters his name and e-mail address and selects "Login as guest"; and
(d) assuming that the customer has previously made a purchase through the Website using the same e-mail address, the customer's contact number and residential address (collectively, the "Personal Data Set") will be displayed on the Guest Checkout Page.

4 Investigations revealed that in relation to (c) above, the Personal Data Set would be displayed upon an exact match with the e-mail address the customer had used previously even if the name entered does not match the name the customer used initially. In the circumstances, the customer's e-mail address was the sole login credential as the "Name" field did not serve any security purpose; access to the Guest Checkout System was not conditional on linking the input entered into the "Name" field with the customer's e-mail address.

5 The Guest Checkout System was launched on 21 April 2014. Data collected from the Guest Checkout System was stored in COURTS' database hosted on the Amazon Web Services server ("AWS Server"). The database contained customers' e-mail addresses, contact numbers and residential addresses.

6 As at 9 July 2017, COURTS confirmed that a total of 14,104 Personal Data Sets were stored in COURTS' database hosted on the AWS Server. The Personal Data Sets belonged to either COURTS' HomeClub customers or to customers who had made a purchase using the Guest Checkout System since 21 April 2014.

7 COURTS took the following remedial actions after it was notified of the Incident:

(a) On 30 August 2017, COURTS launched a new Website with a new Guest Checkout System in place. No data is stored for future use during the new guest checkout process. Customers using the new Guest Checkout System are required to key in their personal data each time a purchase is made. The Guest Checkout Page would not populate the Personal Data Set even if the same customer had previously made a purchase.

(b) On 30 September 2017, COURTS' database containing the Personal Data Sets hosted on the AWS Server was decommissioned.

(c) COURTS engaged a PDPA consultant to conduct PDPA training for its support centre and operation groups, and scheduled a full audit of COURTS' processes.

(d) COURTS put in place additional security measures, such as adopting a policy for penetration tests to be performed at least once every six months on the new Website.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

8 It is not disputed that the Personal Data Set is "personal data" as defined in s 2(1) of the PDPA. There is also no dispute that the PDPA applies to COURTS as it falls within PDPA's definition of "organisation". The issue to be determined by the Commissioner in this case is whether COURTS had complied with its obligations under s 24 of the PDPA.

Whether COURTS complied with its obligations under section 24 of the Personal Data Protection Act

9 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. It is not disputed that COURTS had possession and/or control of the Personal Data Sets stored in COURTS' database, and hosted on the AWS Server. In this regard, COURTS confirmed that Ebee did not have the login credentials to COURTS' database. Its arrangement with Ebee was in the nature of a software development relationship. While the scope of the contract with Ebee covered the maintenance of the Guest Checkout System, in reality,

maintenance was not carried out. COURTS did not engage Ebee to operate the database or perform any form of processing activity on the Personal Data Sets and as such, Ebee was not a data intermediary.

10 The investigations found that COURTS failed to put in place reasonable security arrangements to protect the Personal Data Sets for the following reasons:

(a) E-mail addresses are readily shared by individuals and searchable on various public platforms. The use of an e-mail address as the sole login credential on the Guest Login Page resulting in disclosure of the Personal Data Set on the Guest Checkout Page fell short of the standard of protection required to prevent unauthorised access. As has been held in *Re ABR Holdings Limited*,[2] it is not acceptable to use commonly used identifiers to retrieve personal data. The intention to make the user experience smooth for returning guest shoppers without a HomeClub account was laudable but quite unacceptable as it poses a risk to customers. The entry of an e-mail address was sufficient to retrieve the associated contact number and address that had been stored in the database. This amounted to a failure to protect the personal data of returning customers that falls below the standard expected under the PDPA.

(b) There was a glaring failure by COURTS to adequately consider data protection with respect to the Guest Checkout System of the Website. Although the Website and Guest Checkout Page were launched before the PDPA came into force, COURTS failed to review its system design or process flow, or implement any internal security policies in relation to data protection for the Website after the PDPA came into force for the purpose of ensuring compliance. Additionally,

(i) no penetration tests were conducted since the launch of the Website and the Guest Checkout Page on 21 April 2014;

(ii) no security scans were performed on the Website for a period of 12 months prior to the Incident; and

2 [2017] PDP Digest 117.

(iii) no maintenance of the Guest Checkout System had been carried out since its launch on 21 April 2014.

11 COURTS represented that it had scheduled training programmes in place for all employees with respect to data protection obligations under the PDPA:

(a) new employees are required to go through tailored PDPA training specific to their job scopes during on-boarding; and
(b) PDPA refresher training is conducted for all employees, with the most recent one being in February 2017.

12 While data protection training has an impact on the proper implementation of an organisation's data protection policies and practices, these training measures are ineffective to deal with the system design and process flow deficiencies in the Website and cannot therefore amount to sufficient security arrangements to protect against the unauthorised disclosure of the Personal Data Sets. Admittedly, COURTS conceded that the disclosure of the Personal Data Set on the Guest Checkout Page once an e-mail address matched an existing customers' record in COURTS' database was "an oversight on a design flaw that we were serving data unauthenticated". It is inexcusable for an established organisation like COURTS to neglect its obligations to put in place reasonable security arrangements to protect the Personal Data Sets. This resulted in the Personal Data Sets being exposed to risk of unauthorised disclosure for more than three years.[3]

13 For the reasons above, the Commissioner finds COURTS in breach of s 24 of the PDPA.

THE COMMISSIONER'S DIRECTIONS

14 Given the Commissioner's findings that COURTS is in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to issue COURTS such directions as it deems fit to ensure compliance with the PDPA. This may include directing COURTS to pay a financial penalty of such amount not exceeding S$1m.

3 21 April 2014 to 30 August 2017.

15 In assessing the breach and determining the directions, if any, to be imposed on COURTS in this case, the Commissioner took into account the following aggravating factors:

(a) given that e-mail addresses are widely shared, use of an e-mail address as the sole login credential to protect against unauthorised disclosure of the Personal Data Set was clearly not a reasonable security arrangement;
(b) COURTS subjected the Personal Data Sets to risk of unauthorised disclosure for a substantial period of about three years; and
(c) COURTS displayed a lack of urgency and absence of initiative to obtain information in relation to the Incident.

16 The Commissioner also took into account the following mitigating factors:

(a) there was limited risk of unauthorised disclosure because the Personal Data Set would only be disclosed upon entry of a matching e-mail address used by COURTS' HomeClub customers or previous customers who had made a purchase through the Guest Check Out System;
(b) there was no evidence to suggest any actual loss or damage resulting from the Incident; and
(c) COURTS effected remedial actions upon being informed to implement measures to prevent recurrences of the Incident and to increase employees' awareness of the PDPA.

17 Having considered all the relevant factors of this case, the Commissioner hereby directs COURTS to pay a financial penalty of S$15,000.00 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[4] in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

4 Cap 322, R5, 2014 Rev Ed.

Case Summary

RE HIWIRE DATA & SECURITY PTE LTD

Consent Obligation *– Collection, use and disclosure of personal data without consent – Publicly available data*

13 December 2018

BACKGROUND

1 A complaint was made regarding the Homebiz Information System ("Homebiz") which is a residential and business database offered by the Organisation. The personal data which was allegedly made available through Homebiz comprised 667,338 individuals' full names, race, residential addresses (block numbers, street, unit numbers and postal codes) and telephone or facsimile numbers.

2 The Organisation obtained the personal data of individuals found in Homebiz from publicly available sources such as residential listings ("White Pages") that were published by Global Yellow Pages, the Urban Redevelopment Authority's ("URA") website and other online search results. The race of the individuals was inferred by the Organisation from their names.

ISSUE

3 The issue is whether the Organisation was required to obtain the consent of the individuals concerned under s 13 of the Personal Data Protection Act 2012[1] (the "PDPA") where the personal data was either publicly available or inferred from publicly available data.

1 Act 26 of 2012.

FINDINGS

4 Information obtained from White Pages and the URA website is publicly available as it is "personal data that is generally available to the public". Organisations are not required to obtain the consent of data subjects to collect, use or disclose publicly available personal data.[2]

5 In the circumstances, the Organisation was not required to obtain the consent of the individuals concerned to disclose their full names, residential addresses or telephone or facsimile numbers, as these were obtained from the White Pages or the URA website.

6 The one piece of information which was not found in the White Pages or URA website was the race of the individuals concerned. This was inferred by the Organisation from the name of the individuals. At this juncture, it should be highlighted that personal data which can be easily inferred from publicly available data without much effort or reliance from other sources would also be considered publicly available data. An individual's race may be patently obvious and easily inferred from the name of the individual without much effort or reliance on any other sources.[3]

7 Therefore, the abovementioned personal data is publicly available information under the PDPA and the Organisation was not in breach of s 13 of the PDPA in using or disclosing the personal data.

---

2 As found in para 1(*c*) of the Second Schedule of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA"), para 1(*c*) of the Third Schedule of the PDPA and para 1(*d*) of the Fourth Schedule of the PDPA.

3 If the Organisation had mistakenly inferred the race of the individuals concerned from their names, the Organisation may have been in breach of its s 23 (Accuracy) obligations. Given the absence of any complaints in relation to the accuracy of the information set out in Homebiz Information System, the investigations focused only on the Organisation's compliance with s 13 of the Personal Data Protection Act 2012 (Act 26 of 2012).

MCI (P) 006/07/2019