# PERSONAL DATA PROTECTION DIGEST

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

# PERSONAL DATA PROTECTION DIGEST


**Editor**

Yeong Zee Kin

**Deputy Editors**

David N Alfred

Chen Su-Anne

Justin Blaze George

**Editorial Assistant**

Charis Seow



pdpc

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

2018

CITATION
This volume may be cited as:
[2018] 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) 035/07/2018

# FOREWORD

## BY THE PERSONAL DATA PROTECTION COMMISSIONER

It has been five years since the Personal Data Protection Act 2012 ("PDPA") was enacted and four years since its provisions relating to the protection of personal data came into force. During that time, developments in Singapore and around the world have shown that data protection laws need to keep pace with technological advances, new business models and changes in the expectations of individuals and society at large. As Singapore prepares its economy for a digital future, the Personal Data Protection Commission has embarked on a review of the PDPA with a view to ensuring that our laws are well-suited for the digital economy. The PDPA's stated purpose recognises the rights of individuals to protect their personal data as well as the needs of organisations to collect, use and disclose personal data for appropriate purposes. The Commission is seeking, through its review of the PDPA, to improve the meaningful protection of personal data whilst encouraging innovation in useful data applications by organisations.

This second volume of the *Personal Data Protection Digest* includes several articles which focus on issues of relevance to the digital economy. I am heartened that many data protection practitioners have stepped forward to contribute articles and share their insights into real world data protection issues. This volume also serves to capture some of the prevailing discourse amongst practitioners on various issues. The Commission is cognisant of the range and diversity of views on many aspects of data protection and this is also reflected in the articles in this issue. For example, some of the authors have argued for more rules to better protect personal data while others have weighed in on the side of easing the compliance burden and being more facilitative to business. The Commission encourages practitioners in this field to think more deeply about issues and provides this annual digest as a platform for debate. Well-informed and reasoned discourse by the authors whose contributions are collected in this volume will contribute to a deeper understanding of the concerns and interests which are at the heart of the PDPA.

I hope that you will find the Digest to be informative and thought-provoking whilst you consider your rights and responsibilities as a participant in the digital economy.

**Tan Kiat How**

Commissioner

Singapore

# CONTENTS

## Grounds of Decisions

# PERSONAL DATA PROTECTION COMMISSION'S ENFORCEMENT DECISIONS IN 2017: SOME LESSONS TO BE LEARNT*

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

**Michael CHEN**‡
*JD (Melbourne Law School)*

## I. Introduction

1 The year 2017 saw several important developments in data protection law in Singapore. Chief among them are proposed amendments to the Personal Data Protection Act 2012[1] ("PDPA"), which the Personal Data Protection Commission ("PDPC") sought public consultation on through its issue of a paper on 27 July 2017 entitled "Public Consultation for

* 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, TMT (Technology, Media and Telecommunications)/Data Privacy practice group, Rajah & Tann Singapore. 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* and *The International Who's Who of Telecoms and Media Lawyers*. Steve has been named Communications Lawyer of the Year in the *Corporate Livewire 2015 Legal Awards*. Steve is cited as "one of the best in the field of personal data protection" in Legal 500 2017. Steve is a Certified Information Privacy Professional (Asia) (CIPP/A).

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

1 Act 26 of 2012.

Approaches to Managing Personal Data in the Digital Economy" ("Consultation Paper"). The Consultation Paper portends a mandatory data breach notification regime being put in place and heralds a move away from a strict consent regime as the basis for organisations to process personal data to embrace additional alternative bases for collecting, using and disclosing personal data provided certain conditions are met.

2 On 1 November 2017, the PDPC issued its *Guide to Developing a Data Protection Management Programme*, to assist organisations in complying with the requirements of the PDPA from a policies and practice perspective, and its *Guide to Data Protection Impact Assessments*, to assist organisations in identifying and addressing personal data protection risks.

3 Recognising the sometimes flippant manner in which various organisations have been handling the NRIC numbers of individuals, on 7 November 2017, the PDPC issued a public consultation regarding the proposed revised *Advisory Guidelines on the Personal Data Protection Act for NRIC Numbers*, as well as a proposed *Technical Guide to the NRIC Advisory Guidelines*.

4 These actions are part 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 that they have pro-actively identified and addressed risks to personal data.

5 The slant towards requiring organisations to demonstrate accountability for personal data in their possession or control is further demonstrated by the PDPC's plans to launch a Data Protection Trustmark certification scheme, possibly at the end of 2018.

6 Organisations would also do well to extract key areas of guidance from the PDPC's enforcement decisions. The decisions issued in 2017 provide valuable guidance on the scope of measures that should be taken pursuant to the PDPA's data protection provisions, and the "Protection Obligation" in particular. This article will highlight some pertinent lessons that can be gleaned from some of the 2017 enforcement decisions.

## II. Enforcement decisions issued by the Personal Data Protection Commission in 2017

7 The PDPC remains active in enforcing the PDPA, having issued 19 reported decisions[2] in 2017 (as at the time of writing), as compared to 22 reported decisions in 2016. In these decisions, the organisations in question were punished with financial penalties and/or directions for compliance.

8 A significant majority of the decisions (15 out of the abovementioned 19) 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 "Notification Obligation", "Retention Limitation Obligation" and "Openness Obligation".

9 Most of the cases were initiated by complaints to the PDPC. In several cases, the complainant was not the victim of a personal data breach, but the recipient of another individual's personal data. Where there was a complaint, the majority of the organisations involved were unaware that a breach (or potential breach) of the PDPA had occurred.

10 The specific lessons that can be gleaned from some of the 2017 enforcement decisions will be elaborated on below.

### *A. Protection Obligation – Data intermediaries*

11 If an organisation has acted reasonably and put in place appropriate security measures to protect personal data, it is possible for only the organisation's data intermediary to be held liable in the event of a data breach, and not the organisation.

12 In order for the organisation to be exonerated from the actions or omissions of its data intermediary, it is important and often a precondition to exoneration for the organisation to have executed a written contract with its data intermediary with suitably robust clauses that impose obligations on the data intermediary to protect personal data which the latter is processing on behalf of the primary organisation.

---

2 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.

13 For example, as described in *Re Singapore Telecommunications Limited*,[3] Singapore Telecommunications Limited ("Singtel") had put in place a contract requiring Tech Mahindra (the data intermediary) to comply with the PDPA, adhere to all of Singtel's access and security policies, processes and directions, and ensure that Tech Mahindra's employees were trained to comply with all data protection laws and security measures before it processes personal data on Singtel's behalf.

14 Besides entering into a contract with Tech Mahindra, Singtel took several other measures to ensure that the personal data in its systems were protected. Singtel implemented operational procedures and checks to ensure that Tech Mahindra carried out its functions to protect personal data; conducted annual on-site security reviews of Tech Mahindra's off-site premises as part of its governance process; required Tech Mahindra to confirm its compliance with various security protocols; performed penetration tests on the relevant online systems; and fixed the vulnerabilities that were found. The PDPC accordingly found that Singtel had made reasonable security arrangements in compliance with the Protection Obligation.

15 Hence, having a contract is merely one of the elements that the PDPC would consider in determining whether the primary organisation has done enough to ensure that its data intermediary complies with the PDPA. As seen from the above case, the organisation is expected to have oversight and frequent checks of the data intermediary's processes and practices.

16 The following case elucidates which entity would be viewed as the primary organisation's data intermediary, in a situation where the immediate data intermediary subcontracts part of its personal data processing services to another third party. It also shows that the same analysis would apply regardless of whether parties form part of the same group.

17 In *Re Tiger Airways Singapore Pte Ltd*,[4] Tiger Airways Singapore ("Tigerair") had engaged SATS to perform ground handling services, which involved processing personal data. SATS in turn subcontracted the provision of services to its wholly-owned subsidiary, Asia-Pacific Star

3 [2018] PDP Digest 148.

4 [2018] PDP Digest 166.

("APS"). Accordingly, the PDPC held that both SATS and APS were acting as data intermediaries of Tigerair. The PDPC found that Tigerair had complied with the Protection Obligation because it had imposed suitably worded contractual obligations on SATS to comply with the PDPA. Likewise, SATS had complied with the Protection Obligation because it had imposed suitably worded contractual obligations on APS to comply with the PDPA.

### *B. Protection Obligation – Policies and practices*

18 It is without a doubt that every organisation needs to have appropriately drafted internal data protection policies to assist its staff with compliance with the various data protection obligations in the PDPA.[5]

19 In the case of *Re Management Corporation Strata Title Plan No 3696*,[6] the PDPC espoused the importance of having suitable policies and practices in establishing that an organisation has complied with the Protection Obligation. The following important points can be distilled from this decision:

> (a) Having an overarching internal data protection policy is insufficient for an organisation to meet its obligations under the PDPA to have policies and practices dealing with compliance with the obligations under the PDPA, if such policy is spartan.[7] Hence, organisations must realise by now that this overarching data protection policy needs to significantly deal with the various data protection obligations under the PDPA and explain to staff their ambit so that they may be able to understand and operationalise the same.
>
> (b) The policy should be contextualised to the organisation's operational activities. Hence, it may mean that if the overarching data protection policy does not have enough "meat", in addition to having the said overarching data protection policy, organisations should also have SOPs (standard operating procedures) drafted to deal with

5 *Re Furnituremart.sg* [2018] PDP Digest 175.

6 [2018] PDP Digest 215.

7 See also *Re Furnituremart.sg* [2018] PDP Digest 175.

specific operational activities where significant personal data processing is involved.

20 The *Re Furnituremart.sg*[8] decision further elaborated on the above theme by making clear that in addition to the above, an organisation needs to show that such policies have been implemented and rolled out within the organisation. In other words, just having policies without more, would not be viewed as satisfying the Protection Obligation or the Openness Obligation, as the organisation has to ensure that such policies are indeed operationalised. Further, there also has to be evidence of management having endorsed and requiring implementation of the policies in question. The role that management plays in an organisation's compliance with the PDPA cannot be emphasised enough and it is expected that the PDPC would want to see this theme of PDPA compliance percolating from management to all staff of an organisation.

21 In a group company scenario, it is not uncommon for member organisations of the group to adopt the data protection policy issued by the parent company of the group, as part of their own data protection policy. However, if a group subsidiary company has operational activities specific to it and not the group in general, consistent with the position mentioned above,[9] the PDPC would expect that group subsidiary company to take further steps to contextualise and customise the group level data protection policy to its specific circumstances.[10]

### *C. Protection Obligation – Training, supervision and monitoring*

22 Data protection training may fall under two separate data protection obligations – the Openness Obligation and the Protection Obligation.[11] Under the Protection Obligation, PDPA training may be considered as a type of security arrangement.

23 The PDPC has noted that several foreign data protection authorities, namely, the UK Information Commissioner's Office, Office of the

8 [2018] PDP Digest 175.

9 See para 19(b) above.

10 As was the case for Asia-Pacific Star Private Limited (the subsidiary) in *Re Tiger Airways Singapore Pte Ltd* [2018] PDP Digest 166 at [34].

11 *Re National University of Singapore* [2018] PDP Digest 155 at [21].

Information & Privacy Commissioner for British Columbia, Office of the Privacy Commissioner of Canada, and the Hong Kong Office of the Privacy Commissioner for Personal Data, through their decisions and/or guidance, take the position that data protection training constitutes an important administrative or organisation security measure, and showcases whether an organisation's data protection policies and practices have been appropriately implemented.[12]

24 Even though an organisation may have data protection related policies, having such policies in place without subjecting its staff who handle personal data to appropriate data protection training, would not be sufficient to comply with the Protection Obligation. This means that data protection training is an integral activity that an organisation needs to carry out for its staff, failing which it could be determined that the Protection Obligation has not been complied with. Such training must be regular and can take the form of a traditional classroom setting or through other means such as online training.[13]

25 Each organisation's management plays a crucial role in instilling a culture of security-awareness in that organisation. Therefore, the management of each organisation is expected to establish the standard of care that it expects staff to observe, communicate the relevant policies to staff and train them, and implement appropriate supervision and monitoring to ensure compliance.[14]

### *D. Protection and Retention Limitation Obligations – Review internal processes and systems*

26 Organisations need to review their internal processes and systems involving personal data, in order to minimise the risks that the personal data are compromised or retained for longer than necessary.

27 For example, if personal data are stored on a server which is inadvertently accessible to the public via the Internet, then the organisation needs to evaluate whether the personal data can be promptly deleted once they are no longer in use so as to narrow the window period during which

12 *Re National University of Singapore* [2018] PDP Digest 155.
13 *Re Furnituremart.sg* [2018] PDP Digest 175.
14 *Re Furnituremart.sg* [2018] PDP Digest 175.

there is a risk of unauthorised access, and additionally reduce any risk to personal data in transit, by reducing the frequency of transfers of personal data to that public-facing server.[15]

28 Likewise, data intermediaries should review their systems to determine if personal data are still required to be retained. Data intermediaries beware: if a data intermediary retains personal data it has processed for a primary organisation beyond the service contract required by the primary organisation, or for a longer period than reasonable, where there is no business or legal reason for such retention, then the organisation can no longer be considered a data intermediary in relation to such activities and all of the data protection obligations in the PDPA would apply to such data intermediary and not just the Protection Obligation or Retention Limitation Obligation.[16]

## III. Conclusion

29 In this article, for the sake of brevity, only the pertinent lessons that can be gleaned from some of the enforcement decisions issued by the PDPC in 2017 have been highlighted. Many of these lessons pertain to the Protection Obligation, although it must be borne in mind that many organisations have also been taken to task for breaching other PDPA obligations. The many cases dealing with the Protection Obligation though, reveal that protective measures remain the Achilles' heel for many organisations.

15 *Re Orchard Turn Developments Pte Ltd* [2018] PDP Digest 223.

16 *Re Social Metric Pte Ltd* [2018] PDP Digest 281.

# MANDATORY DATA BREACH NOTIFICATIONS*

**Bryan TAN**†
*LLB (National University of Singapore); Advocate and Solicitor (Singapore), Solicitor (England & Wales)*

**Bernice TIAN**‡
*LLB, BSocSc (Singapore Management University)*

## I. Introduction

1 Under s 24 of the Personal Data Protection Act 2012[1] ("PDPA"), organisations dealing with personal data are required to make "reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". A data breach may occur if such reasonable security arrangements are not put in place or inadequate. Correspondingly, a data breach refers to the *unauthorised* access, collection, use, disclosure, copying, modification, disposal or similar risks of personal data in an organisation's possession or under its control.

2 This article examines the current approach to data breach notification under the PDPA. In line with international developments, this current approach is likely to change. The article therefore further considers the public consultation conducted by the Personal Data Protection Commission of Singapore ("PDPC") in July 2017[2] ("Consultation") and the response paper that followed[3] ("Response"), and the challenges that may

---

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

† Partner, Pinsent Masons MPillay LLP.

‡ Practice Trainee, Pinsent Masons MPillay LLP.

1 Act 26 of 2012.

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

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

arise for organisations in view of the PDPC's intended shift towards a mandatory data breach notification regime.

## II. Application of the current voluntary notification regime

### *A. General approach*

3 Presently, organisations are not obliged to notify affected individuals and/or the PDPC of any data breaches. Nonetheless, under the *Guide to Managing Data Breaches*[4] released by the PDPC, organisations are "advised to notify the PDPC as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals".[5]

4 These voluntary notifications (or the lack thereof) are also taken into consideration when the PDPC determines the penalty to be imposed on an organisation that has breached its PDPA obligations.[6] The PDPC's *Advisory Guidelines on Enforcement of the Data Protection Provisions*[7] ("Enforcement Guidelines") indicates that if the organisation has taken immediate steps to notify affected individuals of the data breach and informed such individuals of the steps they may take to mitigate the risk caused by the data breach, the PDPC may consider it to be a mitigating factor.[8]

5 A review of recent cases indicates that in determining the directions to issue to the organisation following a data breach, the PDPC expressly considers whether the organisation had informed affected individuals of the

4 Issued 8 May 2015.

5 Personal Data Protection Commission, *Guide to Managing Data Breaches* (issued 8 May 2015) at p 10.

6 See Personal Data Protection Commission, *Guide to Managing Data Breaches* (issued 8 May 2015) at p 10.

7 Issued 21 April 2016.

8 See paras 25.3.4–25.3.5 of the Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (issued 21 April 2016).

breach and how such individuals could adopt measures to manage the effects of the leak.[9]

### *B. Sector-specific notification requirements*

6 Depending on the industry that the organisation operates in, it may be subject to other notification requirements that run independently of the PDPA.

7 For instance, financial institutions are obliged to report data breaches to the Monetary Authority of Singapore ("MAS") in certain circumstances. Data breaches must be reported to the MAS if the breach has a severe and widespread impact on the financial institution's operations, or materially impacts the financial institution's service to its customers. Another prominent example can be found in the recently enacted Cybersecurity Act 2018[10] ("CSA"). Under the CSA, owners of computers or computer systems that have been designated as critical information infrastructures are required to notify the Cyber Security Agency in the event of a cybersecurity incident.

8 Since s 4(6) of the PDPA makes it clear that any applicable sector-specific notification requirements are not affected by the organisation's obligations under the PDPA, organisations which are required to notify other regulatory authorities in the event of a data breach would have to do so in addition to any notifications that are made to the PDPC.

## III. Proposed mandatory data breach notification regime

### *A. Criteria for mandatory data breach notification*

9 In its Consultation and Response, the PDPC identified two criteria for an organisation's data breach notification obligation to be triggered. These two criteria are to be applied disjunctively.

---

9 See, *eg*, *Re Singapore Telecommunications Limited* [2018] PDP Digest 148 at [26].

10 Act 9 of 2018.

10 Notably, the PDPC has stated that the organisation's obligation to notify the PDPC under the new mandatory regime will run concurrently with any sector-specific obligations that the organisation may face.[11] Steps will be taken to help streamline the notification process and reduce compliance costs for organisations.[12]

### *(1) Criterion 1: Impact of data breach*

11 Organisations must notify affected individuals and the PDPC of a data breach if the breach is likely to result in significant harm to or have an impact on the individuals to whom the information relates. This would include instances where the data breach involves sensitive personal data like health records or financial information of the affected individuals.[13]

12 The primary rationale for this is to allow affected individuals to take steps to protect themselves from further harm, for instance by changing their passwords or revoking access rights or cancelling their credit cards. Notification to the PDPC is also required so that the PDPC may advise the organisation on the remedial steps to be taken. Over time, the PDPC would also be able to gain a better view of the data protection landscape in Singapore.

13 The language adopted by the PDPC closely resembles that used in Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017 ("Australian Privacy Act"), the provisions of which recently came into force.

---

11 See paras 6.3–6.5 of the Personal Data Protection Commission, "Public Consultation for Approaches to Managing Personal Data in the Digital Economy" (27 July 2017), and paras 11.1–11.4 of the Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in Digital Economy" (1 February 2018).

12 See para 11.4 of the Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in Digital Economy" (1 February 2018).

13 The sensitivity of the personal data involved in a data breach is a factor that the Personal Data Protection Commission takes into account when determining the direction to issue to an organisation. See *Re Singapore Telecommunications Limited* [2018] PDP Digest 148 at [26] and *Re JP Pepperdine Group Pte Ltd* [2017] PDP Digest 180 at [22].

Under the Australian Privacy Act, notification to affected individuals is required if the breach is likely to result in serious harm to the individual. Similar criteria have also been applied in other jurisdictions.[14] The European Union's General Data Protection Regulation ("EU GDPR"), for instance, requires organisations to communicate a data breach to affected individuals if the breach is likely to result in a high risk to the rights and freedoms of the individuals.[15]

*(2) Criterion 2: Scale of data breach*

14 Organisations must notify the PDPC of any data breaches that occur on a significant scale. Given the large number of affected individuals, the PDPC does not require the organisation to notify the PDPC unless the nature of the data concerned is such that the data breach would *also* be likely to result in significant harm to or impact on the affected individuals.

15 In the Consultation, the PDPC had proposed using data breaches involving 500 affected individuals as the benchmark of a significant scale that would require notification to be made to it. However, the PDPC has since indicated in its Response that it will not impose a statutory threshold to determine the scale of impact. Further guidance on assessing the scale of impact will be provided in the PDPC's guidelines.

16 The implementation of this criterion is based on the view that data breaches of significant scale would be more likely to require investigation and/or intervention by the PDPC. In this way, the PDPC would be better placed to offer guidance to the organisation on the appropriate remedial actions it should take. The use of this criterion is thus in line with the PDPC's current approach, under which the amount of personal data compromised is expressly taken into account when determining the directions and penalties to be issued to the organisation in question.[16]

17 It is important to note that the significant scale threshold operates independently of the other significant harm or impact criterion that requires the organisation to notify the affected individuals – it would still

14 See s 26WE of the Australian Privacy Act 1988.

15 See Art 34 of the European Union General Data Protection Regulation.

16 See *Re K Box Entertainment Group Pte Ltd* [2017] PDP Digest 1 at [42]–[43].

have to notify the affected individuals even if the significant scale threshold is not met.

### *B. Technological protection exception*

18 Under the technological protection exception, organisations will be exempted from the requirement to notify affected individuals if the data that were lost had been encrypted to a reasonable standard, such that the data would be illegible. The technological protection exception can also be found in the EU GDPR.[17]

19 The rationale for this exception is that in the event of a data breach, any personal data acquired by the unauthorised person would be unusable or illegible unless they were decrypted by the unauthorised person. Consequently, the organisation may be treated as having discharged its protection obligation under s 24 of the PDPA to make reasonable security arrangements to protect the personal data that it deals with.

20 The scope and application of this exception is also in line with the PDPC's current approach under the voluntary notification regime. Putting in place passwords or other mechanisms to prevent unauthorised access is a mitigating factor that is to be considered when the PDPC decides the organisation's penalty following a data breach.[18] The complexity of the protection is also relevant – encoded passwords may be insufficient to satisfy the protection obligation under s 24 of the PDPA if the passwords are encoded with a commonly used cryptographic hash function which could be deciphered easily.[19]

---

17 Article 34(3) of the European Union General Data Protection Regulation exempts an organisation from notifying affected individuals if the organisation has "implemented appropriate technological and organisational protection measures … to the personal data affected by the personal data breach, in particular those that would render the personal data unintelligible to any person who is not authorised to access it".

18 See para 25.3.2 of the Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (issued 21 April 2016).

19 See *Re Fei Fah Medical Manufacturing Pte Ltd* [2017] PDP Digest 28 at [19]–[20].

### C. *Law enforcement exception*

21 Under the law enforcement exception, organisations which have suffered an eligible data breach are exempted from notifying affected individuals if the breach is the subject of an ongoing or potential investigation and the notification to those affected individuals is likely to impede that investigation. Following the Response, the ambit of the law enforcement exception has been expanded to include investigations by agencies that are authorised by law.

22 The law enforcement exception serves to ensure that the data protection interests of individuals are balanced against the public interest of promoting justice. A similar exception is provided for under the Australian Privacy Act. The Australian Commissioner may exempt organisations from notifying affected individuals of a data breach for a period of time to prevent compromising an investigation into the data breach, or if such notification would be likely to lead to further eligible data breaches.[20]

### D. *Remedial action exception*

23 In its Response, the PDPC also indicated that it intends to provide an exception for organisations that have taken remedial actions to reduce the potential harm to or impact on the affected individuals. The remedial action exception will only apply if the organisation can show that the result of their remedial actions is that the breach is not likely to cause any significant harm to or impact on the affected individuals.

24 This newly-proposed exception is also in line with the PDPC's current approach to data breach cases. Under the Enforcement Guidelines, it is a mitigating factor if the organisation has engaged meaningfully with the affected individuals to voluntarily offer them remedies and methods of reducing the harm that would befall these individuals as a result of the breach. Cases also indicate that the remedial actions adopted by an organisation following a breach (or lack thereof) are expressly taken into

20 Section 26WQ of the Australian Privacy Act 1988 permits the Privacy Commissioner to exempt organisations from notifying affected individuals of data breaches, having regard to any relevant advice from law enforcement agencies.

account as a factor when the PDPC determines the directions to be given to the organisation.[21]

## IV. Cross-border issues

25 Although the shift towards a mandatory data breach notification regime in Singapore is a move that largely follows developments in other jurisdictions, there are certain cross-jurisdictional issues that may arise for organisations who operate across territorial boundaries. For instance, an organisation may suffer a data breach in one country where the data are stored, but there are affected individuals in other countries. It may also be the case that the affected personal data in the organisation's possession are stored across various countries. The key question for such organisations to consider is: in which country/countries should a notification be made?

26 The issue is made more pertinent by the fact that the data protection rules in different countries are similar, but not identical. Unlike other areas of law such as trade or intellectual property, there has yet to be an international harmonisation of personal data protection standards. The shift towards adopting a mandatory data breach notification regime has been a fairly new – and gradual – one. Most jurisdictions have only very recently implemented such rules or are still in the midst of introducing these rules to their data protection legislation.[22] The vast majority of countries, however, do not have explicit statutory requirements to notify the relevant authority and/or affected individuals in the event of a data breach.

27 Even where the relevant countries all have mandatory data breach notification obligations, the standards required to trigger the obligation and/or to fall within any relevant exceptions may be different. For instance, while both Australia and California have mandatory data breach notification regimes, the California Civil Code requires notification to affected individuals whose unencrypted personal information was obtained

21 See *Re Social Metric Pte Ltd* [2018] PDP Digest 281 at [37] and *Re Fei Fah Medical Manufacturing Pte Ltd* [2017] PDP Digest 28 at [34].

22 For instance, the mandatory data breach notification rules in Australia only came into effect on 22 February 2018, while the European Union General Data Protection Regulation will only become enforceable on 25 May 2018. New Zealand, like Singapore, is currently exploring the inclusion of a mandatory data breach notification requirement to its data privacy laws.

by an unauthorised person,[23] whereas the Australian requirement is triggered only where there is likely to be serious harm to the affected individuals.[24]

28 In the absence of an international standard for data protection laws, the cross-jurisdictional issues highlighted above are unlikely to be addressed by regulators. Organisations whose business operations involve a cross-border element would do well to ensure that their internal policies are able to manage this in order to minimise the negative effect of enforcement actions by authorities in different countries. For instance, given the relatively short time period in which notification is due to take place for an eligible breach, the organisation's data breach crisis management policies – or at least, the designated data protection officer – should ensure that information about the extent of the organisation's cross-border operations is readily available. This would include information as to the data protection and notification laws of countries in which a data breach may be possible, as well as an awareness of where the organisation's clients may be located and the data protection laws therein. The relevant countries' authorities should be notified within the respective timeframes, in order not to fall foul of the mandatory notification obligation.

29 Following notification, the organisation should endeavour to ensure that it engages in prompt communication with all the relevant regulatory authorities, to prevent authorities from forming the impression that the organisation is not addressing the situation with sufficient gravity.[25] At the same time, remedial measures should be taken on an organisational level to address the fallout from the breach and improve protection measures. Undertaking remedial action is now all the more important given that this step is no longer viewed merely as a mitigating factor in the assessment of the PDPC's penalties, but may exempt the organisation from its notification obligation, and consequently, any public relations fallout that accompanies notifying affected individuals of the data breach that the organisation has suffered.

---

23 See California Civil Code § 1798.29(a) and § 1798.82(a).

24 See s 26WE(2) of the Australian Privacy Act 1988.

25 See *Re Social Metric Pte Ltd* [2018] PDP Digest 281 at [37] and *Re Singapore Telecommunications Limited* [2018] PDP Digest 148 at [26].

## V. Conclusion

30 The creation of an obligation to notify the PDPC and/or affected individuals of a data breach is a significant update to the PDPA. Both affected individuals and the PDPC will now receive prompt notifications in the event of a data breach, enabling the former to take protective measures and the latter to recommend remedial action. However, events following the Consultation and Response in relation to the data disclosed in the Facebook and Cambridge Analytica case show that mandatory breach notification, while not being able to prevent breach, would at least go some way to mitigate some of the effects of the data breach. While the recentness of the proposed changes means that there has yet to be clear guidelines from the PDPC on the practical application of these rules, organisations dealing with personal data whose operations go beyond the geographical boundaries of Singapore should be aware of the potential challenges that have been identified here. Such organisations would do well to ensure that their internal processes are updated and ready for the shift towards a mandatory data notification regime across a number of jurisdictions, and take steps to ensure their compliance with the data protection laws of each country.

# PROTECTION OF SENSITIVE PERSONAL DATA*

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

## I. Introduction

1 The Personal Data Protection Act[1] ("PDPA") recognises the right of individuals to protect their personal data.[2] As the PDPA establishes a comprehensive data protection regime, it protects all types of personal data and it generally does not discriminate among different types of personal data.[3] However, where sensitive personal data are concerned, the Singapore data protection regime justifiably adopts a more protective stance.

2 It is generally accepted that sensitive personal data merit stronger protection. Across jurisdictions, a basic principle of data protection laws is that "the processing of certain types of data that are regarded as especially sensitive for data subjects should be subject to more stringent controls than other personal data".[4] Established data protection frameworks such as those of the European Union, Canada, the UK, Australia and Hong Kong afford special protection to sensitive personal data, although the way in which this special protection is conferred differs among jurisdictions.

3 The notion of sensitive personal data is not a new one in Singapore.[5] In 1990, the Law Reform Committee proposed a data protection system

---

* 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.

† Teaching Assistant, National University of Singapore.

1 Act 26 of 2012.

2 Personal Data Protection Act (Act 22 of 2012) s 3.

3 This is subject to a number of exceptions. For example, business contact information is not protected.

4 Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press, 2014) at p 165.

5 See Benjamin Wong, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012" (2017) 7(4) *International Data Privacy Law* 287 for a brief overview of the historical development of data protection law in Singapore.

that distinguished between sensitive and non-sensitive personal data, imposing different rules on data users depending on whether they dealt with sensitive personal data or not.[6] Later, the 2002 Model Data Protection Code for the Private Sector explicitly granted additional protection to sensitive personal data in its data protection principles.[7]

4 This article examines Singapore's current approach to the protection of sensitive personal data.[8] In the main, two questions will be addressed. First, when are personal data considered sensitive? Second, what are the practical implications when personal data are considered sensitive?

## II. When are personal data considered sensitive?

### *A. Categories of sensitive personal data*

5 As a starting point, the PDPA does not legislatively define sensitive personal data. This is unlike the approach adopted in the European Union General Data Protection Regulation,[9] which defines certain special categories of personal data (*eg*, personal data revealing political opinions or religious beliefs) over which added protection is conferred.

6 Despite the absence of an express legislative definition of sensitive personal data, however, the Singapore data protection framework does recognise the concept of sensitive personal data. In particular, the advisory guidelines and decisions of the Personal Data Protection Commission ("PDPC") make frequent reference to the concept of sensitivity. In the recent decision of *Re Aviva Ltd*,[10] the PDPC set out a list of types of

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

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

8 See also Simon Chesterman, *Data Protection in Singapore: Privacy and Sovereignty in an Interconnected World* (Singapore: Academy Publishing, 2014) at para 1.60–1.62.

9 Regulation (EU) 2016/679.

10 [2018] PDP Digest 245.

personal data which, in its view, would "typically be more sensitive in nature":[11]

> … NRIC/Passport numbers; personal data of a financial nature such as bank account details, Central Depository account details, securities holdings, transaction and payment summaries; names of the policyholder's dependents or beneficiaries, the sum insured under the insurance policy, the premium amount and type of coverage; an individual's personal history involving drug use and infidelity; sensitive medical conditions; and personal data of minors.

7 The abovementioned list in *Re Aviva Ltd* was made on the basis of "past decisions and advisory guidelines".[12] This suggests an incremental approach towards the concept of sensitive personal data: rather than being exhaustively defined, the concept of sensitive personal data is kept open to subsequent accretion and evolution. The implication of this incremental approach is that the list in *Re Aviva Ltd* does not represent a closed class of sensitive personal data. Future decisions and guidelines may be expected to add to, or subtract from, that class.

### *B. Sensitivity as potential for harm*

8 An incremental approach necessitates clarity on how the sensitivity of personal data is to be assessed, so that it is possible to determine what personal data are sensitive. Are there objective criteria that determine whether a particular piece of personal data is sensitive? There does not appear to be a conclusive answer to this question. However, there does appear to be support for a harm-based analysis, *viz*, the greater the potential for harm occasioned by its improper collection, use or disclosure, the more sensitive the personal data.

---

11 *Re Aviva Ltd* [2018] PDP Digest 245 at [17]. This is not an exhaustive list: see Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised on 28 March 2017) at para 3.14, where "records of adopted children and their biological parents" are classified as highly sensitive personal data.

12 *Re Aviva Ltd* [2018] PDP Digest 245 at [17].

9 For example, in *Re Management Corporation Strata Title Plan No 3696*,[13] the PDPC considered that NRIC numbers were generally of a sensitive nature "as it is widely used for business purposes and transactions with the Government, and could be used to cause harm should such information fall into the wrong hands".[14] In *Re Aviva Ltd*,[15] the PDPC stated that insurance details were sensitive "not only from a financial perspective but can also be socially embarrassing" (suggesting that harm in this context includes non-economic harm).[16] Similarly, in *Re Credit Counselling Singapore*[17] it was stated in no uncertain terms that an individual's financial information relating to their debt status was sensitive personal data, and that:[18]

> 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.

10 A harm-based understanding of sensitivity is consistent with the list of sensitive personal data set out in *Re Aviva Ltd*.[19] The types of personal data in that list could, if improperly used or disclosed, result in significant harm to the individuals to which they relate. Identifiers such as NRIC and passport numbers may be exploited to perpetrate identity fraud; individuals' histories of social deviancy may adversely affect their relationships, reputations and economic prospects, particularly if they are made known to others in the absence of context; certain medical conditions continue to attract social stigma; minors may be made more vulnerable to grooming and other dangers if their personal details are exposed to predators. The list of sensitive personal data is therefore explicable by a harm-based conception of sensitivity.

---

13 [2018] PDP Digest 215.

14 *Re Management Corporation Strata Title Plan No 3696* [2018] PDP Digest 215 at [10].

15 [2017] PDP Digest 107.

16 *Re Aviva Ltd* [2017] PDP Digest 107 at [38].

17 [2018] PDP Digest 295.

18 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [19].

19 [2018] PDP Digest 245.

11 The harm-based analysis also provides the normative basis for the enhanced protection of sensitive personal data. In other words, data protection law is justified in being more protective over sensitive personal data because of the potential for harm that could arise from their improper collection, use or disclosure, the potential for harm being usually greater than would be the case if the personal data were non-sensitive.

12 Despite the observations made above, it should be stressed that at this juncture, the above-stated relationship between sensitivity and the potential for harm is inferential. A more conclusive position must await future developments in this aspect of the Singapore data protection framework.

## III. What are practical implications when personal data are considered sensitive?

### *A. Implications on fulfilment of data protection obligations*

13 Where an organisation possesses, controls or processes sensitive personal data, the sensitivity of that personal data bears implications on what the organisation must or must not do in order to comply with its data protection obligations. Two data protection obligations, in particular, may be so affected: the "Protection Obligation" and the "Purpose Limitation Obligation".

#### *(1) Protection Obligation*

14 Under the Protection Obligation, an organisation is obliged to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.[20]

15 In general, the more sensitive the personal data, the higher the level of security that should be afforded to that personal data. In its *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, the PDPC states that organisations should "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels

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

of sensitivity".[21] This was emphasised in *Re Aviva Ltd*,[22] where the PDPC agreed with the view of the Office of the Privacy Commissioner of Canada 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'".

16 In a similar vein, it was maintained in *Re Credit Counselling Singapore* that:[23]

> When it comes to the protection of sensitive personal data, there is a need to put in place stronger security measures because of the actual or potential harm, and the severity of such harm, that may befall an individual from a misuse or unauthorised use of such data.

17 The higher standard of care for sensitive personal data has been reflected in the PDPC's decisions.[24] For example, in *Re Ang Rui Song*,[25] a financial consultant was held to have breached the Protection Obligation due to his improper disposal of his clients' insurance documents. On the facts, the financial consultant had simply put the documents into a plastic bag and placed the bag into a trash bin, which meant that the documents remained readable. This was found to be "inappropriate given the sensitivity of the information found in the documents, such as the policy holder's name, NRIC number, premium amounts, name of life assured, benefits and sums assured, and maturity date".[26] The PDPC held that the documents should have been shredded, with the level of shredding "guided by the level of sensitivity of the personal data contained in the document".[27]

---

21 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at para 17.3.

22 [2018] PDP Digest 245 at [19].

23 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [25].

24 See, *eg*, *Re ABR Holdings Limited* [2017] PDP Digest 117 at [16]; *Re JP Pepperdine Group Pte Ltd* [2017] PDP Digest 180 at [17] and *Re Tiger Airways Singapore Pte Ltd* [2018] PDP Digest 166 at [34].

25 [2018] PDP Digest 236.

26 *Re Ang Rui Song* [2018] PDP Digest 236 at [21].

27 *Re Ang Rui Song* [2018] PDP Digest 236 at [21].

*(2) Purpose Limitation Obligation*

18 Under the Purpose Limitation Obligation, 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.[28]

19 It is submitted that the Purpose Limitation Obligation may be stricter when sensitive personal data are involved. This is because the Purpose Limitation Obligation incorporates a consideration of all the circumstances of each case, and it is at least plausible that the sensitivity of the personal data constitutes a relevant "circumstance".

20 More specifically, there appears to be some support for the proposition that sensitive personal data should only be collected, used or disclosed where *necessary* for a reasonable purpose – it is not sufficient that the collection, use or disclosure was merely *relevant* to the purpose. In other words, sensitive personal data should not be collected, used or disclosed for a purpose if that purpose could be accomplished by alternative means.

21 The necessity standard is justifiable in the context of sensitive personal data. In fulfilling their data protection obligations, organisations are expected to act as a reasonable person would consider appropriate in the circumstances.[29] In view of the risks to individuals where sensitive personal data are concerned, it is reasonable to expect organisations to adopt alternatives to collecting, using or disclosing sensitive personal data, unless such collection, use or disclosure is necessary.

22 The necessity standard was applied in *Re Naturally Plus Singapore Pte Limited*,[30] where the PDPC held that an organisation had not breached the Purpose Limitation Obligation in collecting photocopies of the front of individuals' credit cards and NRIC/Work Permits, for the purpose of identity verification and authentication. In its reasoning, the PDPC considered whether there were alternative means of fulfilling that purpose "given the sensitivity of the personal data involved", and concluded that other forms of identification would not be adequate.

23 The necessity standard also features in the PDPC's *Proposed Advisory Guidelines on the Personal Data Protection Act for NRIC Numbers*

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

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

30 [2017] PDP Digest 230.

("NRIC Guidelines"). Among other matters, the proposed NRIC Guidelines provides for a restriction that, in general, organisations should not collect, use or disclose an NRIC number or NRIC copy unless the collection, use or disclosure is (a) required under the law or (b) necessary to accurately establish and verify the identity of the individual.[31] While the proposed NRIC Guidelines does not expressly refer to the Purpose Limitation Obligation in imposing the restriction, it is submitted that the Purpose Limitation Obligation is the logical legal basis for the restriction, since the restriction specifies the purposes for which NRIC numbers and NRIC copies may be collected, used and disclosed. If this reading is correct, then the proposed NRIC Guidelines in fact specifies how the Purpose Limitation Obligation is fulfilled in relation to NRIC numbers and NRIC copies, by (a) prescribing the purposes for which NRIC numbers and NRIC copies may be collected, used or disclosed and (b) requiring that the collection, use or disclosure be necessary for those purposes.

24 To conclude, it may be helpful to formulate the necessity standard in the terms of the legislative wording of the Purpose Limitation Obligation, as follows. The Purpose Limitation Obligation permits the collection, use or disclosure of personal data only for purposes that a reasonable person would consider appropriate in the circumstances. While a purpose may *prima facie* seem appropriate in the abstract, it may not be appropriate in the light of the circumstances, in particular where the personal data are sensitive and the collection, use or disclosure is not necessary for that purpose.

### *B. Implications on financial penalties*

25 The PDPA provides that a financial penalty not exceeding $1m may be imposed on organisations who breach their data protection obligations.[32] The sensitivity of the personal data involved in a breach is a relevant consideration in the assessment of the financial penalty to be imposed for that breach.

---

31 Personal Data Protection Commission, *Proposed Advisory Guidelines on the Personal Data Protection Act for NRIC Numbers* at para 1.5.

32 Personal Data Protection Act (Act 26 of 2012) s 29(2)(*d*).

26 In its *Advisory Guidelines on Enforcement of the Data Protection Provisions*, the PDPC states that it is an aggravating factor that the organisation concerned:[33]

> … is in the business of handling [a] large volume of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to a person (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of that personal data.

27 The PDPC's decisions take into account the sensitivity of personal data in the assessment of financial penalties. In *Re DataPost Pte Ltd*,[34] "a significant aggravating factor" was that sensitive personal data were disclosed by the data breach, "warranting a financial penalty as a matter of general deterrence". It is interesting to note that sensitivity was the sole aggravating factor in that case – it remains to be seen whether this aggravating factor will consistently be sufficient grounds for imposing financial penalties for data breaches, as a deterrent policy.

28 In contrast, in cases where the breach involved personal data that were not sensitive, the non-sensitivity of the personal data was considered a mitigating factor.[35]

## IV. Conclusion

29 In sum, Singapore's approach to the concept of sensitive personal data may be characterised as a "non-legislative category-based approach", which provides non-legislative but definite categories of sensitive personal data. This approach permits the incremental refinement of those categories, enabling the Singapore data protection framework to adjust to changes in the economic and social context. Where personal data are sensitive, stronger protection is granted by way of a stricter application of the data protection obligations, and higher penalties for breaches of those obligations.

30 As businesses continue to discover innovative ways to exploit personal data, both organisations and individuals should be awake to the risks

---

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

34 [2018] PDP Digest 207 at [19].

35 See for example *Re Furnituremart.sg* [2018] PDP Digest 175 at [29].

attendant to such exploitation where sensitive personal data are involved. In particular, the unauthorised disclosure of an individual's sensitive personal data may have long-lasting detrimental effects on the welfare of that individual, by exposing them to identity theft or by inflicting damage on their reputation and relationships, among other harms.

# RELEVANCE OF DATA PROTECTION IN COMPETITION ASSESSMENTS*

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

## I. Introduction

1 Whilst data protection[1] law and competition law are separate areas of law which promulgate different aspects of consumer protection, the application of both areas of law may overlap in certain circumstances.

2 This article will seek to examine the interaction between data protection and competition law through the following three perspectives:

(a) the interaction between competition law, data protection and big data;

(b) whether the provision of personal data to the Competition Commission of Singapore[2] ("CCS"), the statutory authority that

---

* 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.

† 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*, and has been endorsed for his excellence in regulatory work: *Practical Law Company's Which Lawyer Survey: Who's Who Legal: TMT and Who's Who Legal: Competition*.

1 Whilst there has been extensive debate on the conceptual differences between "data protection" and "privacy", for expediency, this article uses the terms "data protection" and "privacy" interchangeably, based on the prevailing terminology used in the particular jurisdiction being discussed.

2 Now known as the Competition and Consumer Commission of Singapore (as amended by the Enterprise Singapore Board Act 2018 (Act 10 of 2018) wef 1 April 2018).

administers and enforces the Competition Act,[3] may raise issues under the Personal Data Protection Act 2012[4] ("PDPA") in the following circumstances:

(i) when required by law; or

(ii) for the purposes of a voluntary notification; and

(c) whether the provision of personal data to third parties, such as economists, legal counsel and other advisers, for the purposes of conducting market assessments, may raise issues under the PDPA.

## II. Interaction between competition law, data protection and big data

3 It is currently accepted that "data is increasingly being recognised as an asset to businesses" and capable of bringing about a wide range of benefits to businesses and consumers.[5] However, for its benefits to be fully realised, it is necessary to ensure that businesses do not engage in anti-competitive conduct in the course of embracing big data.

4 The issue of data and data protection has arisen in a series of decisions relating to the competitiveness of market conduct of major technology companies that seek to leverage on big data. This section will briefly touch on the following situations:

(a) whether a merger involving datasets may lead to substantial lessening of competition in the relevant markets; and

(b) whether it is possible for the collection, use and/or disclosure of data to lead to market foreclosure.

5 It is acknowledged that the starting position for all collection, use and disclosure of data (especially personal data) is the need for an organisation to obtain valid consent from the individuals affected. To the extent that such consent has been obtained, the organisation may collect, use and/or disclose such data for the purposes covered by the individual's consent. This may include purposes such as allowing the organisation to use such data for

3 Cap 50B, 2006 Rev Ed.

4 Act 26 of 2012.

5 Competition Commission of Singapore Occasional Paper, "Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights" (16 August 2017) at p 5.

the purposes of improving its services and to show more relevant advertising. Competition law steps in when, notwithstanding such consent being obtained, the market conduct of the organisation with respect to the data collected, used and/or disclosed, or the method by which the organisation does so, raises potential anti-competitive concerns.

6 In such situations, various competition authorities have considered that data protection law and related issues can be taken into account "if only as an element of context" when conducting a competition law analysis.[6] Such a situation may arise when a dominant undertaking implements data protection/privacy policies for data which serve as a main input of its products and/or services. In these cases, "there may be a close link between the dominance of the company, its data collection processes and competition on the relevant markets, which could justify the consideration of privacy policies and regulations in competition proceedings".[7] The CCS has also stated that privacy policies can be a factor in the competition assessment if it is relevant to non-price competition. For example, where "privacy is something which affects the quality of a service delivered, the treatment of personal data may affect how [the] CCS considers and assesses the competitive dynamics of a specific market".[8]

7 In the discussion that follows, it is interesting to note when data and data protection law become relevant to a competition assessment.

8 Turning first to mergers involving datasets, mergers involving non-complementary datasets have generally been found not to lead to a substantial lessening of competition.

9 First, in the case of Facebook's acquisition of Whatsapp in 2014, the European Commission ("EC") analysed "potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof", and concluded that "only Facebook, and not WhatsApp, is active in the provision of online

---

6 Bundeskartellamt & Autorité de la concurrence, "Competition Law and Data" (10 May 2016) at p 23.

7 Bundeskartellamt & Autorité de la concurrence, "Competition Law and Data" (10 May 2016) at p 24.

8 Competition Commission of Singapore Occasional Paper, "Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights" (16 August 2017) at para 216.

advertising services" and "since WhatsApp does not currently collect any user data that are valuable for advertising purposes, the Transaction does not increase the amount of data potentially available to Facebook for advertising purposes". Given the absence of complementary datasets, the acquisition was cleared.

10 Notably, this transaction was notified to the US Federal Trade Commission ("FTC") and the EC, and both authorities cleared the transaction. In clearing the transaction, the FTC wrote to the parties reminding them of their continuing obligations under privacy law[9] and the EC stated as follows:[10]

> Any privacy-related concerns flowing from the increased concentration of data … do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.

11 Second, in the case of *Google/DoubleClick*,[11] whilst Google and DoubleClick were considered to be both active in the online ad serving industry, the EC and the FTC cleared the merger unconditionally, deciding that Google and DoubleClick were not close, actual or potential competitors in any markets for online advertising or services. It was considered that Google is present in the market for the provision of online advertising space while DoubleClick does not sell advertising space, and the parties do not directly compete in the market for the provision of display ad serving technology.[12] Further, whilst DoubleClick and Google may technically have complementary datasets, the EC found (amongst others) that:

> (a) the information that DoubleClick had was "relatively narrow in scope" as compared to other companies active in online advertising;

---

9 Letter from Jessica L Rich, Director, Bureau of Consumer Protection, Federal Trade Commission, to Erin Egan, Chief Privacy Officer, Facebook, Inc and Anne Hoge, General Counsel, WhatsApp Inc (10 April 2014) <https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf> (accessed 3 January 2018).

10 *Case No COMP/M.7217 – Facebook/WhatsApp* at para 164.

11 *Case No COMP/M.4731* – Google/DoubleClick.

12 *Case No COMP/M.4731* – Google/DoubleClick at para 192.

(b) DoubleClick was contractually prohibited from using data it had collected from existing customers to offer better targeting to new advertiser customers, since the data belonged to existing customers;

(c) the merged dataset was already available to several competitors or could be purchased from third parties; and

(d) even after the merger, there was no concern about the cross-use of data by the merged entity because it would be extremely difficult for it to impose "far-reaching" contractual changes on its customers, in the light of factors such as DoubleClick lacking market power to do so or customers potentially switching to other ad serving providers instead.

12 In the light of this, the EC did not block the merger and stated that:[13]

> This Decision refers exclusively to the appraisal of this operation with Community rules on competition … In any event, this Decision is without prejudice to the obligations imposed onto the parties by Community legislation in relation to the protection of individuals and the protection of privacy with regard to the processing of personal data …

13 Likewise, the FTC released a statement that privacy considerations alone are not a basis to block or impose conditions on a merger where they do not constitute a non-price attribute of competition.[14]

14 Unlike mergers involving non-complementary datasets, the outcome of mergers involving complementary datasets tends to be slightly more complicated. In such cases, competition concerns relate to whether the potential concentration of data may lead to a substantial lessening of competition. Such substantial lessening of competition may arise from portfolio effects, which come about when firms operating in different product markets (and therefore not competitors) merge and, as a result of the merger, gain control of complementary goods such that they become incentivised to engage in anti-competitive conduct like tying or bundling.

---

13 *Case No COMP/M.4731 – Google/DoubleClick* at para 368.

14 Federal Trade Commission, "Statement Concerning Google/DoubleClick" FTC File No 071-0170, at p 2 <https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf> (accessed 3 January 2018).

15 In the *Microsoft/LinkedIn* decision,[15] the complementarity between customer data and customer relationship management ("CRM") software solutions was considered. Microsoft provides CRM software solutions, but LinkedIn does not. However, LinkedIn offers sales intelligence solutions, which can provide (at the very least) "basic information about potential points of contact for sales generation", and is therefore complementary to Microsoft's CRM software solutions. LinkedIn's Sales Navigator draws upon LinkedIn's database of 430 million profiles, of which 105 million are actively maintained. A market study conducted also revealed that "privacy is an important parameter of competition and driver of customer choice in the market for [professional social network] services".[16]

16 Given the complementarity of the products involved, the EC raised some preliminary competition concerns. In its eventual clearance of the transaction, the EC took into consideration the commitments provided by Microsoft (aimed at addressing the potential competition concerns that the EC may have had) and the fact that "Microsoft is subject to European data protection laws which limit its ability to undertake any treatment of LinkedIn full data" and while the then-prevailing LinkedIn "privacy policy allows [it] to share the personal data it collects, processes, stores and uses with its controlling companies, this is only for the purposes described in the privacy policy itself".

17 Also of interest was the EC's clarification on the role of data protection-related considerations in competition assessments, which signalled a shift from its previous position in the Facebook/Whatsapp merger:[17]

> Privacy related concerns … can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor.

18 Turning next to whether it is possible for the collection, use and/or disclosure of data to lead to market foreclosure such as to trigger abuse of

---

15 *Case No M.8124 – Microsoft/ LinkedIn*.

16 *Case No M.8124 – Microsoft/ LinkedIn* at fn 330.

17 European Commission Press Release, "Mergers: Commission Approved Acquisition of LinkedIn by Microsoft, Subject to Conditions" (6 December 2016) <http://europa.eu/rapid/press-release_IP-16-4284_en.htm> (accessed 3 January 2018).

dominance concerns, competition concerns could arise if access to big data constitutes an "essential facility" for access to certain digital markets.[18] A particular data set is regarded as an "essential facility" where it is indispensable to other players, and there are no alternative products. Restricting access to such an "essential facility" imposes technical, legal and economic obstacles that make it impossible or unreasonably difficult to compete in the downstream market, thus likely resulting in the foreclosure of competition. However, challenges arise in determining whether personal data held by a dominant company is intended to erect a barrier to entry against competitors, or whether it is legitimately held as part of the dominant company's business model.

19 Under certain circumstances, abuse of dominance concerns may arise due to an undertaking's method of collecting data as part of its efforts to harness big data. This is illustrated by the preliminary assessment by the German Federal Cartel Office ("FCO") that Facebook's method of amassing user information to build up an accurate targeted advertising profile constitutes an abuse of dominance due to the "exploitative business terms" imposed by Facebook on its users.

20 In this case, it was considered that Facebook was abusing its dominance by requiring consumers to consent to the collection of all types of user data from third-party websites, and its subsidiaries such as WhatsApp and Instagram. Facebook generally collects data on the way consumers use third-party websites, and subsequently incorporates that data by merging it with the user's Facebook profile to build up a more accurate targeted advertising profile. When a Facebook user views a page which has a Facebook "Like" button embedded in it, a record of the page view is made, and associated with the user's Facebook account, even if the user does not click the "Like" button.[19] This was held by the FCO to be an abuse of Facebook's dominant position, given the pervasiveness of Facebook in the lives of Germans, the lack of options that a user who does not consent to such collection has with respect to their usage of Facebook, and the fact that

18 European Data Protection Supervisor's Preliminary Opinion of March 2014 at para 40.

19 Reuters, "Facebook Abused Dominant Position, Says German Cartel Office" *CNBC* (19 December 2017).

access to personal data is a criterion for market power under the German Competition Act, especially for online platforms and networks.

21 In the wake of the FCO's action against Facebook, commentators have queried whether such an action could be "wrongly paternalistic"; "whether consumers know or not what terms and conditions they are accepting may be a public policy issue, but one that … is not for competition law to address".[20]

## III. Provision of information containing personal data to the Competition Commission of Singapore and other third parties for competition assessments

22 Moving on from how data protection may become relevant to competition assessments, this section will look at how the provision of information containing personal data to the CCS and other third-party service providers in connection with competition filings could potentially raise certain issues under the PDPA.

### *A. Situations where information containing personal data is provided to the Competition Commission of Singapore*

#### *(1) Overview of the Competition Commission of Singapore and its powers*

23 Broadly, the three activities prohibited (collectively, "Prohibitions") under the Competition Act are:

(a) agreements, decisions and practices which prevent, restrict or distort competition;[21]
(b) abuse of a dominant position;[22] and
(c) mergers that substantially lessen competition.[23]

---

20 See Chillin' Competition at <https://chillingcompetition.com/2016/03/02/facebook-privacy-and-article-102-a-first-comment-on-the-bundeskartellamts-investigation/> (accessed 7 January 2018).

21 Competition Act (Cap 50B, 2006 Rev Ed) s 34.

22 Competition Act (Cap 50B, 2006 Rev Ed) s 47.

23 Competition Act (Cap 50B, 2006 Rev Ed) s 54.

24 In administering and enforcing the Competition Act, the CCS has the power to investigate and adjudicate anti-competitive activities, including the imposition of financial penalties on infringing parties. The powers of the CCS as enshrined in the Competition Act are as follows:

(a) The CCS may conduct an investigation in so far as there are reasonable grounds for suspecting that any of the Prohibitions has been infringed.[24]

(b) The CCS may, in the course of investigation or conducting a study of the market, require any person to produce specified documents and/or information to it.[25]

(c) The CCS may enter premises without a warrant (written notice of at least two working days to be given of its intended entry).[26]

(d) The CCS may enter and search premises with a warrant (*ie*, dawn raids).[27]

(e) The CCS may enter into agreements with other sectoral regulators to co-operate in cross-sectoral competition cases, which may include information sharing between the regulators.[28]

25 These powers may be exercised not only against the undertakings suspected of infringement, but also third parties including complainants, suppliers, customers and competitors.

26 Some examples of the documents that the CCS may look at include electronically-stored documents and e-mails, business cards and correspondence (both electronic and physical).

*(2) Provision of information voluntarily*

27 Apart from the provision of information to the CCS as a result of the CCS exercising its investigative powers or in response to its requests for information, there are potentially two other situations where information (which may include personal data) may be voluntarily provided to the CCS:

---

24 Competition Act (Cap 50B, 2006 Rev Ed) s 62.
25 Competition Act (Cap 50B, 2006 Rev Ed) ss 61A and 63.
26 Competition Act (Cap 50B, 2006 Rev Ed) s 64.
27 Competition Act (Cap 50B, 2006 Rev Ed) s 65.
28 Competition Act (Cap 50B, 2006 Rev Ed) s 87.

(a) whistleblowing reports that are submitted to the CCS; and

(b) under the voluntary notification regime for mergers in Singapore.[29]

### *B. Whether provision of information to the Competition Commission of Singapore will raise issues under the Personal Data Protection Act*

#### *(1) Introduction*

28 It should be noted that the CCS, as a public agency, is exempt from the PDPA. However, public sector data protection rules based broadly on the same data protection principles as the PDPA continue to apply to the CCS.

#### *(2) Provision of information as required by law*

29 An organisation is exempted from obtaining consent where the collection, use or disclosure of the individual's personal data is required or authorised under the PDPA or any other written law.[30] Written law is defined in the Interpretation Act[31] as "the Constitution and all previous Constitutions having application to Singapore and all Acts, Ordinances and enactments by whatever name called and subsidiary legislation made thereunder for the time being in force in Singapore".[32] Accordingly, where information is provided by an organisation to the CCS pursuant to the exercise of the CCS's investigative powers, as provided for under the Competition Act, the organisation will be exempted from the consent obligation.

---

29 Competition Commission of Singapore, *Guidelines on Merger Procedures 2012* – Form M1.

30 Section 13 of the Personal Data Protection Act 2012 (Act 26 of 2012) states that "consent is required unless the collection, use or disclosure … without the consent of the individual is required or authorised under this Act or any other written law".

31 Cap 1, 2002 Rev Ed.

32 Interpretation Act (Cap 1, 2002 Rev Ed) s 2(1).

*(3) Provision of information voluntarily*

30 Unlike the preceding category of information provision, the exception from the consent obligation as provided above is generally inapplicable to information containing personal data that are *voluntarily* provided by an organisation to the CCS. This is because such information is not required by any written law *per se*.

31 Notwithstanding this, other exceptions may potentially apply depending on the specific facts and circumstances. For example, it may be possible to argue that disclosure pursuant to the whistleblowing report would fall within the exception to consent set out under para 1(*g*) of the Fourth Schedule to the PDPA, in so far as the disclosure is to a public agency (in this instance, the CCS), and such disclosure is necessary in the public interest.

32 Also, an organisation need not seek the consent of the individual to whom the personal data relates if the disclosure of personal data is necessary for any investigation or proceedings. Under the PDPA, "investigation" means an investigation relating to:[33]

> (a) a breach of an agreement;
>
> (b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
>
> (c) a circumstance or conduct that may result in a remedy or relief being available under any law;

33 In a whistleblowing submission to the CCS, it is arguable that any personal data disclosed pursuant to the whistleblowing report would fall under limb (b), given that whistleblowing would involve a breach of the Competition Act such as to trigger some form of investigation by the CCS.

34 In a case where an organisation voluntarily notifies its conduct to the CCS for a decision on whether the undertaking's conduct contravenes any competition law,[34] it is similarly arguable that any personal data disclosed pursuant to the CCS's queries would fall under limb (b) above such that no consent needs to be obtained from the individual to whom the personal data relates prior to the disclosure. That said, the situation is less

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

34 Competition Act (Cap 50B, 2006 Rev Ed) s 44 or 51.

straightforward if such personal data are provided at the initial stage of the application given that there is no clarity on whether an investigation would be commenced.

35 As at the time of writing, consent will likely be required where personal data are provided at such an initial stage. Notably, however, in its "Public Consultation for Approaches to Managing Personal Data in the Digital Economy" issued on 27 July 2017 ("Public Consultation"), the Personal Data Protection Commission ("PDPC") recognised that there may be circumstances in which an organisation may need to collect, use or disclose personal data without consent for a legitimate purpose, but such collection, use or disclosure is not authorised under the PDPA or other written law; for instance, the sharing and use of personal data to detect and prevent fraudulent activities.[35] After reviewing all of the feedback, the PDPC confirmed in its "Response to Feedback on the Public Consultation" on 1 February 2018 ("Response to Feedback"), that it intends to provide for "Legitimate Interests", as a basis to collect, use or disclose personal data regardless of consent.[36]

36 Such "Legitimate Interests" exception is intended to cater for situations where there is a need to protect legitimate interests which will have economic, social, security or other benefits for the public (or a section thereof), but where it is unlikely that the individuals whose personal data are proposed to be collected, used and/or disclosed will provide their consent (*eg*, to avoid fraud detection).

37 To rely on this exception, an organisation will need to conduct a risk and impact assessment to determine whether the benefits of the collection, use and/or disclosure without consent outweigh the foreseeable adverse impact to the affected individual. In addition to this, an organisation must also:

(a) disclose its reliance on this exception as a ground for collection, use or disclosure; and

---

35 Personal Data Protection Commission, "Public Consultation for Approaches to Managing Personal Data in the Digital Economy" (issued 27 July 2017) at para 3.14.

36 Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy" (issued 1 February 2018) at para 5.6.

(b) make available a document justifying its reliance on this exception, together with the business contact information of the person responsible for responding to any questions from the individuals affected.

38 Ultimately, a case-by-case assessment will be required to determine if an organisation contemplating a notification to the CCS is entitled to rely on the upcoming "Legitimate Interests" exception. Nevertheless, it is conceivable that this exception will come in handy especially in cases where (a) there is genuine uncertainty as to whether a widespread practice is anti-competitive, and (b) the personal data involved are crucial to the determination of this question.

### *C. Situations where information containing personal data is provided to third parties, such as economists and legal counsel, for purposes of conducting competition assessments*

39 In the ordinary course of competition assessments conducted for the purposes of applying for merger clearances[37] or notifications for decisions (or guidance) in respect of potential infringements of ss 34 and/or 47 of the Competition Act, an organisation would often engage third-party external advisers to render opinions or draft submissions based on the information furnished to them. It is not inconceivable that such information provided to third parties by an organisation may occasionally contain personal data.

40 In these situations, a data protection issue that may arise relates to whether valid consent has been sought from the relevant individuals prior to the disclosure of their personal data to such external advisers for the purposes of conducting the relevant assessments.

41 Whilst the PDPA contains exceptions to the consent obligation, such as where "the personal data is publicly available",[38] where the collection, use or disclosure is necessary for "any investigation or proceedings",[39] or "for

37 Competition Act (Cap 50B, 2006 Rev Ed) s 57.

38 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*c*); Third Schedule, para 1(*c*) and Fourth Schedule, para 1(*d*).

39 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule para 1(*e*); Third Schedule, para 1(*e*) and Fourth Schedule, para 1(*f*).

evaluative purposes",[40] these apply to narrow situations and rarely suffice for the purposes of obtaining external competition advice.

42 For example, if one examines the exception which applies where "the personal data is used for a research purpose, including historical or statistical research",[41] it might at first glance appear to include the disclosure of information containing personal data to the external adviser, given that such adviser would arguably be conducting some form of research into the market. However, this is further qualified by more stringent conditions, such as the following, amongst others, without which consent would still have to be obtained:

> (a) the research purpose cannot reasonably be accomplished without the personal data being provided in an individually identifiable form;
> (b) it is impracticable for the organisation to seek the consent of the individual for the disclosure;[42] and
> (c) the personal data will not be used to contact persons to ask them to participate in the research.[43]

43 Given the limited nature of the exception, an organisation seeking third-party advice and disclosing information for this purpose would be well advised to seek the necessary prior consents from the affected individuals beforehand. Alternatively, if the personal data contained within the information disclosed to such third-party advisers is unnecessary for the purposes of the competition assessment, such documents should be anonymised and the personal data redacted prior to disclosure.

44 Further, as a matter of general prudence and as part of the protection obligation, organisations should also ensure that the third-party advisers to

---

40 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*f*); Third Schedule, para 1(*f*) and Fourth Schedule, para 1(*h*).

41 Personal Data Protection Act 2012 (Act 26 of 2012) Third Schedule, para 1(*i*) and Fourth Schedule, para 1(*q*).

42 When assessing whether it would be "impracticable" for an organisation to seek consent of the individual, the specific facts of the case will have to be considered: see "Practical Guidance to Queries by Medical Research Institution" issued by the Personal Data Protection Commission on 25 August 2016.

43 Personal Data Protection Act 2012 (Act 26 of 2012) Third Schedule, para 2 and Fourth Schedule, para 4.

whom information is disclosed have in place proper secure processes to safeguard the data received by them. If necessary, appropriate data transfer agreements should be entered into between the organisation and its third-party advisers.

## IV. Conclusion

45 This article has sought to explore the potential overlaps between data protection and competition laws from two main angles:

(a) first, by tracing how data protection/privacy may be taken into consideration when competition assessments are conducted; and

(b) second, by identifying the common scenarios where information containing personal data may be disclosed in connection with matters involving competition law. In this regard, two situations were covered, namely, where the information is disclosed to the CCS and where information is disclosed to third-party advisers, such as economists or legal counsel.

46 Following the rising prevalence of big data, data protection issues are likely to gain more prominence in the conduct of competition analysis and it remains to be seen how these issues will eventually develop. Ultimately, data protection and competition laws should collectively serve to better total welfare, whilst simultaneously being cautious not to batter or discourage pro-competitive conduct.

# INTRICACY OF AND INTERPLAY BETWEEN DATA PROTECTION AND CYBERSECURITY*

**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)*

## I. Introduction

1 In today's globalised and technologically-enhanced world, personal data are stored in many different places, to wit, cloud[1] (*eg*, Amazon Web Services), computer (*eg*, files and e-mails) and portable storage media for

---

* This article was written in the author's personal capacity and whose views do not in any way represent the views or policy positions of the Personal Data Protection Commission. All errors remain the author's own.

† Team Lead, Investigations Unit (Data Protection and Do Not Call), Personal Data Protection Commission; Adjunct Lecturer, Singapore Management University School of Law; Guest Lecturer, National University of Singapore Faculty of Law. Lanx is also one of the authors of *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, forthcoming) and had spoken at various conferences and seminars such as Data Privacy Asia, IAPP Asia Privacy Forum, IAPP KnowledgeNet and NUS CLE Seminar Series. The author would like to express his utmost gratitude to Yeong Zee Kin for his patient guidance and invaluable comments. The author would also like to acknowledge Dr Vivienne Yu, Nicholas Fong and Yvette Anthony for proofreading this article.

1 Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*eg*, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. See Peter Mell & Timothy Grance, "The NIST Definition of Cloud Computing" (2011) *National Institute of Standards and Technology Special Publication 800-145*.

cost efficiency and convenience. Naturally, data protection shares an intimate relationship with cybersecurity (including computer misuse), and many data breaches in Singapore[2] and overseas[3] concern unauthorised access or hacking activities that have resulted in data leakage. In her pursuit to become a smart nation,[4] develop the digital economy[5] and be a favoured global data hub,[6] Singapore clearly understands that she needs to correspondingly ensure that organisations[7] provide adequate security and data protection for system, network, server and data storage to prevent data breaches and cybersecurity incidents. In this regard, the Computer

2 See, *eg*, *Re K Box Entertainment Group Pte Ltd* [2017] PDP Digest 1; *Re The Institution of Engineers Singapore* [2017] PDP Digest 18; *Re Fei Fah Medical Manufacturing Pte Ltd* [2017] PDP Digest 28; *Re Metro Pte Ltd* [2017] PDP Digest 57; *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 and *Re Orchard Turn Developments Pte Ltd* [2018] PDP Digest 223.

3 See, *eg*, Nate Lord, "A Timeline of the Ashley Madison Hack" *Digital Guardian* (27 July 2017); Sam Thielman, "Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History" *Guardian* (15 December 2016); Robert Hackett, "LinkedIn Lost 167 Million Account Credentials in Data Breach" *Fortune* (18 May 2016) and Nick Hopkins, "Deloitte Hit by Cyber-Attack Revealing Clients' Secret Emails" *Guardian* (25 September 2017).

4 Tan Teck Boon, "In Smart Nation Drive, S'pore Must Strengthen Personal Data Protection" *The Straits Times* (2 March 2016).

5 Commissioner of the Personal Data Protection Commission, Tan Kiat How, mentioned at the PDP Seminar 2017 that the "Digital Economy provides exciting opportunities for businesses and workers … seen the rise of platforms in domains such as e-commerce, social media and e-payments, and the growth of vibrant digital ecosystems around these platforms … A robust data protection regime is important to engender trust in our ecosystem and enable our companies to seize growth opportunities". Available at <https://www.pdpc.gov.sg/pdpc/news/press-room/2017/07/address-by-mr-tan-kiat-how-commissioner-of-pdpc> (accessed 10 January 2018).

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

7 The author notes the different terminologies employed under the Personal Data Protection Act 2012 (Act 26 of 2012) and the Cybersecurity Bill. In this regard, the terms organisation, business entity, owner and company will be used interchangeably, unless otherwise highlighted.

Misuse Act[8] ("CMA") was amended on 3 April 2017,[9] the Cybersecurity Act 2018[10] was passed in Parliament on 5 February 2018[11] and the Personal Data Protection Act 2012[12] ("PDPA") is currently undergoing its first major review.[13]

2 Many write-ups tend to provide a broad discussion in relation to the similarities and differences between the concepts of privacy (including data protection) and cybersecurity.[14] This article, however, seeks to articulate the relationship, and delineate the boundary between the two areas of law in the Singapore context.[15] In particular, it focuses on the potential overlap of jurisdictions between the PDPA, the Cybersecurity Act and the CMA, and how such overlap is resolved under the PDPA.

---

8 Cap 50A, 2007 Rev Ed. Formerly known as the Computer Misuse and Cybersecurity Act; the name was a consequential change due to the passing of the Cybersecurity Act 2018 (Act 9 of 2018). See Irene Tham, "Cyber-Security Czar Can Get Confidential Info for Probes" *The Straits Times* (6 February 2018).

9 Kevin Kwang, "Changes to Singapore's Cybercrime Law Passed" *Channel NewsAsia* (3 April 2017).

10 Act 9 of 2018.

11 See Jalelah Abu Baker, "Cybersecurity Bill Passed in Parliament; MPs Raise Questions on Privacy, Cost" *Channel NewsAsia* (5 February 2018) and Irene Tham, "Cyber-Security Czar Can Get Confidential Info for Probes" *The Straits Times* (6 February 2018). It has been noted that the Cybersecurity Act 2018 (Act 9 of 2018) has yet to come into effect at the time of this article.

12 Act 26 of 2012.

13 Tan Weizhen, "Informing Customers of Breaches among Proposed PDPA Changes" *Today* (27 July 2017).

14 See, *eg*, Rick Robinson, "Data Privacy vs Data Protection" *Defrag This* (8 March 2016) <https://blog.ipswitch.com/data-privacy-vs-data-protection> (accessed 10 December 2017); Dsguaman, "Privacy vs Data Protection vs Information Security" *Blog* (1 November 2016) <http://blogs.upm.es/sse/2016/11/01/privacy-vs-data-protection-vs-information-security/> (accessed 9 December 2017) and Francoise Gilbert, "Privacy v Data Protection. What is the Difference?" *Francoisegilbert.com* (1 October 2014) <https://www.francoisegilbert.com/?p=937> (accessed 10 December 2017).

15 Due to the word limit, this article does not attempt to provide an overview of the Personal Data Protection Act (Act 26 of 2012), Cybersecurity Act 2018 (Act 9 of 2018) and Computer Misuse Act (Cap 50A, 2007 Rev Ed), nor address the full extent of the synergy and overlap between them.

## II. Cybersecurity Act and Personal Data Protection Act

3 Many a time, a data breach is due to the security of a computer system, network, server or data storage being compromised. When such an incident occurs, an organisation may find itself subject to multiple legal obligations in Singapore. This may not be ideal for the organisations or authorities concerned (*ie*, the Cyber Security Agency ("CSA") or the Personal Data Protection Commission ("PDPC")). For these organisations, there is the potential increase in cost and manpower required to manage a data or security breach.[16] Similarly, the PDPC would want to avoid expending unnecessary resources to investigate the same matter as there is the likelihood that its jurisdiction may be subsequently precluded under s 4(6)(*b*) of the PDPA, which states that 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*.[17] In this instance, the PDPC may refuse to conduct an investigation under s 50(3)(*d*) of the PDPA.[18]

16 For example, the need to notify or duplicity in the process of engaging multiple authorities.

17 There is also the potential issue of double jeopardy but that will not be examined in this article. See, *eg*, Gary Chan Kok Yew, "Prosecutorial Discretion and the Legal Limits" (2013) 25 SAcLJ 15 at paras 23–25 and Eric Tan & Jessica Soo, "Fundamental Liberties in Disciplinary Inquiries" *SMA News* (April 2013) at pp 40–41. In gist, parallel actions taken by the Cyber Security Agency under the Cybersecurity Act 2018 (Act 9 of 2018) and the Personal Data Protection Commission under the Personal Data Protection Act 2012 (Act 26 of 2012) are unlikely to be considered as double jeopardy since the former is a criminal offence and the latter is regulatory in nature. That said, although the principle of double jeopardy under Art 11(1) of the Constitution of the Republic of Singapore (1999 Rev Ed) only applies when a person is charged with the same criminal offence (in fact and law) twice, it is conceivable that neither the Personal Data Protection Commission nor the Cyber Security Agency would want to find the same organisation in breach if the same set of facts give rise to liabilities under the Personal Data Protection Act and the Cybersecurity Act. See also *Re Wee Harry Lee* [1983–1984] SLR(R) 274 endorsing the House of Lords' decision in *Connelly v Director of Public Prosecutions* [1964] AC 1254, and s 244 of the Criminal Procedure Code (Cap 68, 2012 Rev Ed).

18 See *Re Ocean Front Pte Ltd* [2017] PDP Digest 216. See also *Re My Digital Lock Pte Ltd* [2018] PDP Digest 334.

This is to prevent the risk of there being inconsistent requirements imposed by the different regulators.[19]

### *A. Parties concerned*

#### *(1) Cybersecurity Act*

4 Under s 3 of the Cybersecurity Act, the CSA has the jurisdiction to investigate any organisation that has been designated as a *critical information infrastructure*[20] ("CII") by the Commissioner of the CSA[21] in the event that the owner of the CII has failed to: (a) adhere to the codes of practice and standards of performance[22] under s 11(6) of the Cybersecurity Act, (b) establish such mechanisms and processes for the purposes of detecting cybersecurity threats and incidents under s 14(2) of the Cybersecurity Act, or (c) conduct cybersecurity audits[23] and risk assessments[24] as required by s 15(1) of the Cybersecurity Act. In relation to s 11(6), the CSA Commissioner may direct an organisation to comply with

19 See also *Report on Public Consultation on the Draft Cybersecurity Bill* issued by the Ministry of Communications and Information and the Cyber Security Agency of Singapore (13 November 2017) at para 14.

20 Critical information infrastructure is defined in the First Schedule to the Cybersecurity Act 2018 (Act 9 of 2018) as any services relating to energy, info-communications, water, healthcare, banking and finance, security and emergency, aviation, land transport, maritime, government and media.

21 See s 7 of the Cybersecurity Act 2018 (Act 9 of 2018). See also *Report on Public Consultation on the Draft Cybersecurity Bill* issued by the Ministry of Communications and Information and the Cyber Security Agency of Singapore (13 November 2017) at para 18.

22 The codes of practice or standards of performance may be issued by the Commissioner of the Cyber Security Agency from time to time under s 11(1) of the Cybersecurity Act 2018 (Act 9 of 2018). At the time of this article, the author notes that the Commissioner has yet to issue any codes of practice or standards.

23 At least once every two years as required under s 15(1)(*a*) of the Cybersecurity Act 2018 (Act 9 of 2018).

24 At least once a year as required under s 15(1)(*b*) of the Cybersecurity Act 2018 (Act 9 of 2018).

the code of practice or standard of performance.[25] Failure to comply with the aforesaid direction will attract a fine not exceeding $100,000 or to imprisonment for a term not exceeding two years or to both under s 12(6) of the Cybersecurity Act.[26] Likewise, non-compliance with ss 14(2) and 15(1) carries the same penalties under ss 14(3) and 15(7)(*a*).[27]

5 The legal obligations imposed on CII owners, however, do not apply to computer systems in the supply chain supporting the operation of a CII. For example, a third-party vendor that supports the business of a CII will not be deemed as an owner of a CII. On this subject, the CSA and its parent ministry (the Ministry of Communications and Information) have clarified that CII owners are ultimately responsible for the cybersecurity of their CIIs and they should consider imposing cybersecurity requirements on their vendors via contracts, if necessary.[28]

6 Nonetheless, the CSA has the power to prevent and investigate cybersecurity incidents or serious cybersecurity incidents in respect of any computer or computer systems in Singapore (*ie*, not limited to CII).[29] Under s 19 of the Cybersecurity Act, the CSA can investigate cybersecurity incidents to assess the potential impact or impact of a cybersecurity incident, or prevent further harm or another cybersecurity incident from the initial cybersecurity incident.[30] The CSA can also investigate a cybersecurity incident which satisfies the severity threshold under s 20 of the Act. A serious cybersecurity incident is classified as one that creates a

25 See s 12(2)(*b*) of the Cybersecurity Act 2018 (Act 9 of 2018).

26 In the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction. See s 12(6) of the Cybersecurity Act 2018 (Act 9 of 2018).

27 Cybersecurity Act 2018 (Act 9 of 2018) s 15(7)(*a*). In the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

28 *Report on Public Consultation on the Draft Cybersecurity Bill* issued by the Ministry of Communications and Information and the Cyber Security Agency of Singapore (13 November 2017) at paras 7 and 10.

29 Daniel Song, "What You Need to Know about Singapore's New Cybersecurity Bill" *Bird & Bird* (26 July 2017).

30 *Report on Public Consultation on the Draft Cybersecurity Bill* issued by the Ministry of Communications and Information and the Cyber Security Agency of Singapore (13 November 2017) at para 26.

risk of significant harm to a CII, risk of disruption to the provision of an essential service,[31] creates a threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, or the cybersecurity threat or incident is of a severe nature regardless whether it involves a CII.[32]

### *(2) Personal Data Protection Act*

7 In relation to the PDPA, organisations which are in possession or control of personal data will be subject to the nine obligations set out under the PDPA, *viz*, the consent obligation, purpose limitation obligation, notification obligation, access and correction obligations, accuracy obligation, protection obligation, retention limitation obligation, transfer limitation obligation and openness obligation.[33] Unlike the Cybersecurity Act, a third party (*ie*, data intermediary) which processes personal data on behalf of another organisation shall be liable under the protection and retention obligations.[34]

8 The discussion herein will concentrate on the protection obligation under s 24 of the PDPA, as it is the obligation that most relates to security breaches.[35] For example, in *Re K Box Entertainment Group Pte Ltd*[36] ("*Re K Box*"), the data breach incident involving the disclosure of more than 350,000 members' personal data was caused by weaknesses in relation to the organisation's access control (*eg*, weak password policy), weak control

---

31 Critical information infrastructure is defined in the First Schedule to the Cybersecurity Act 2018 (Act 9 of 2018) as any services relating to energy, info-communications, water, healthcare, banking and finance, security and emergency, aviation, land transport, maritime, government and media.

32 See s 20(3) of the Cyber Security Act 2018 (Act 9 of 2018).

33 See ss 11–26 and 32 of the Personal Data Protection Act 2012 (Act 26 of 2012). See, *eg*, Tan Sin Liang, "How Well Do You Understand the Personal Data Protection Act and its Practical Implications" *Singapore Law Gazette* (April 2014).

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

35 For other examples, see *Re The Institution of Engineers Singapore* [2017] PDP Digest 18; *Re Fei Fah Medical Manufacturing Pte Ltd* [2017] PDP Digest 28; *Re Metro Pte Ltd* [2017] PDP Digest 57 and *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160.

36 [2017] PDP Digest 1.

over unused accounts, and the organisation's *failure to conduct audits of its security system*. In the same vein, in *Re Orchard Turn Developments Pte Ltd*[37] ("*Re Orchard Turn*"), an unknown perpetrator with an Egyptian IP address had gained unauthorised access to Orchard Turn's servers, and sent phishing e-mails to 24,913 members of the organisation. Orchard Turn could not pinpoint the source of the likely leak of credentials, and identify the person who had accessed the system.

### *(3) Convergence*

9 *Prima facie*, an organisation that is designated as a CII by the Commissioner of the CSA under s 7 of the Cybersecurity Act, and has personal data in its possession or control,[38] will be subject to both the Cybersecurity Act and the PDPA. To illustrate this point – if the organisations in *Re K Box* and *Re Orchard Turn had been CII owners*, they could have been in breach of the Cybersecurity Act for failing to establish such mechanisms and processes for the purposes of detecting cybersecurity threats, and for failing to conduct cybersecurity audits (besides their breach of the protection obligation under the PDPA). Hypothetically, it is likely that the PDPC would not have initiated investigations against K Box or Orchard Turn under ss 4(6) and 50(3)(*d*) of the PDPA, as the CSA would have been the more appropriate authority since cybersecurity protection is a matter of national interest.

10 That said, in both cases, the security weaknesses in K Box and Orchard Turn's computer systems were also attributed to their vendors, Finantech and Super-E. Finantech was found liable under s 24 of the PDPA whereas Super-E was not simply because it was considered to be out of the PDPA's jurisdiction (but it would have been liable under s 24 if that were not the case). Ergo, the PDPC can investigate and/or take action against Finantech and Super-E, but the CSA would not be able to as the Cybersecurity Act does not extend to vendors of CII owners for the obligations under ss 11, 14 and 15 of the Cybersecurity Act.

11 Notwithstanding the above, the CSA has the authority to investigate and prevent cybersecurity or serious cybersecurity incidents under ss 19

37 [2018] PDP Digest 223.

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

and 20 of the Cybersecurity Act so long as the computer or the computer system is located in Singapore. In this regard, conceivably, the legislative intent of the provisions is to enable the CSA to investigate the root causes of the cybersecurity incident, to remedy it and to prevent proliferation.[39] The aforesaid will run parallel with the protection obligation under s 24 of the PDPA where the PDPC may investigate whether the organisation has put in place reasonable security measures to protect the computer or computer system that contains the personal data.[40] In the event that the organisation has failed to do so, the PDPC could impose a financial penalty and/or direct the organisation to undertake certain action to prevent future recurrence.[41] The PDPC and the CSA may impose similar directions when it comes to remedial or preventive measures.

12 Concomitantly, this will bring us to the next discussion in relation to data breach notification, as both the CSA and PDPC need to be notified promptly, in order to avoid the situation where one proceeds to investigate the matter without the knowledge of the other and issue duplicative directions to an organisation to remediate the cybersecurity and data breach incident.

### *B. Notification of breaches*

13 Under s 14(*a*) of the Cybersecurity Act, an organisation has the obligation to report to the CSA: (a) a prescribed cybersecurity incident in respect of the CII; (b) a prescribed cybersecurity incident in respect of any computer or computer system that is interconnected with or that communicates with the CII; and (c) any other type of cybersecurity incident in respect of the CII that the Commissioner of the CSA has specified by written direction to the organisation. An owner could be fined not exceeding $100,000 or be imprisoned for a term not exceeding two years or to both under s 12(6) of the Cybersecurity Act for non-performance.

---

39 Cybersecurity Act 2018 (Act 9 of 2018) s 20(2)(*b*).

40 There could also be a concurrent breach of the Computer Misuse Act (Cap 50A, 2007 Rev Ed) on the part of the hacker if he has criminal intent but this will be explored later in this article.

41 Personal Data Protection Act 2012 (Act 26 of 2012) s 29.

14 Currently, there is no breach notification requirement under the PDPA. Nonetheless, based on past precedents,[42] it has been duly noted that the PDPC does consider prompt data breach notification by organisations as a mitigating factor when calibrating the amount of financial penalty to be imposed. Further, the PDPC intends to prescribe mandatory notification requirements[43] under its present review of the PDPA. From this aspect, moving forward, an organisation would need to inform both the CSA and PDPC if a security breach involves (a) a CII, or (b) computer or computer system in Singapore, and (c) personal data. Until then, the PDPC relies on the CSA or other sectoral regulators to notify it of a potential data breach, subject to their respective preservation of secrecy provisions.[44]

15 The obligation to report a cybersecurity breach to multiple authorities is always a cause of concern for many businesses,[45] as it will increase the costs of doing business and duplicate efforts. This is especially the case if the authorities are asking for similar information. As such, an organisation may want to prepare a single set of notification documents that contain facts that would be required by the multiple authorities, that is, summary of the incident, cause of the breach, type of personal data compromised, date of incident, number of people affected, remedial actions taken, *etc*. As discussed above, it is possible that the PDPC will not investigate security and data breaches that involve a CII owner, but it can do so against the vendor in such cases. In like manner, the PDPC is unlikely to investigate a security and data breach if the CSA has investigated and directed the CII,

---

42 See, *eg*, *Re Central Depository (Pte) Limited* [2017] PDP Digest 81; *Re Aviva Pte Ltd* [2017] PDP Digest 107 and *Re Singapore Telecommunications Limited* [2018] PDP Digest 148.

43 See Rachelle Lee, "Privacy Watchdog Proposes Mandatory Notification for Certain Data Breaches" *Channel NewsAsia* (27 July 2017) and "Majority of Responses 'Supportive' of Mandatory Breach Notification: PDPC" *Channel NewsAsia* (1 February 2018).

44 See s 3 of the Cybersecurity Act 2018 (Act 9 of 2018) and s 59 of the Personal Data Protection Act 2012 (Act 26 of 2012). See also *Report on Public Consultation on the Draft Cybersecurity Bill* issued by the Ministry of Communications and Information and the Cyber Security Agency of Singapore (13 November 2017) at para 23.

45 *Report on Public Consultation on the Draft Cybersecurity Bill* issued by the Ministry of Communications and Information and the Cyber Security Agency of Singapore (13 November 2017) at para 6.

computer or computer system owner to rectify the security breach under s 12 or 20 of the Cybersecurity Act.

16 This leaves the last question: Who has jurisdiction over the hacker who caused the security and/or data breach?

## III. Computer Misuse Act

17 More often than not, a security and data breach incident would involve a hacker. In this vein, the actions of the hacker are governed under the CMA. This has been affirmed by the Minister for Communications and Information, Dr Yaacob Ibrahim, during the parliamentary debate of the Cybersecurity Bill.[46] On the other hand, the responsibility to protect the computer or computer system, or personal data lies with the organisations under the Cybersecurity Act or the PDPA.[47] If an organisation misuses personal data, it could potentially fall within the ambit of both the CMA and the PDPA.

18 Under s 8(1) of the CMA, it is an offence if someone discloses or accesses access codes (a) for any wrongful gain, (b) for an unlawful purpose, or (c) knowing that it is likely to cause wrongful loss to any person. At the same time, it is a breach of the protection obligation under s 24 of the PDPA if an organisation fails to put in place reasonable protection to protect the personal data in its possession or under its control. In *Re The Institution of Engineers Singapore*,[48] personal data (60,000+ telephone numbers, and 6,000+ *member IDs and passwords*) of Institution of Engineers Singapore ("IES") members had been posted on Pastebin. IES was found to be in breach of s 24 of the PDPA for failing to put in place adequate measures and security to protect its members' personal data.

19 However, the individual who disclosed the *access code* on Pastebin for a non-commercial purpose would only be liable under s 8(1) of the CMA,[49]

---

46 Irene Tham, "Cyber-Security Czar Can Get Confidential Info for Probes" *The Straits Times* (6 February 2018).

47 This article will only examine the relationship between the Personal Data Protection Act 2012 (Act 26 of 2012) and the Computer Misuse Act (Cap 50A, 2007 Rev Ed).

48 [2017] PDP Digest 18.

49 In the event that he is being located and charged by the police.

and not the PDPA. This is because the PDPA does not cover an individual who acts in a personal capacity if he or she undertakes activities for his or her own purposes (see 4(1) of the PDPA and para 6.9 of the PDPC's Advisory Guidelines on Key Concepts in the Personal Data Protection Act).[50]

20 In the same way, s 8A(1) of the CMA makes it an offence for a person who, knowing that personal information was obtained in breach of the CMA, either (a) transfers it to another knowing that that other will use it to commit an offence, or (b) obtains or retains it with a view to such transfer in the future or to himself for the purpose of committing an offence. The transferor in this case is in breach of s 8A(1) of the CMA, if he knows that the personal information was *obtained in contravention* of the CMA, and proceeds to transfer or sell that personal information. Further, if the transferor carries on the business of selling or using such personal information, there is a potential breach of the consent and notification obligations[51] under the PDPA for unauthorised disclosure and use, even if he is an individual.[52] As discussed above, when such overlap arises, the PDPC may exercise its discretion under s 50(3)(*d*) of the PDPA and defer to the jurisdiction of the Singapore Police to investigate and charge the individual under s 8A(1) of the CMA. This is because the PDPC focuses on the lack of protection by businesses as opposed to going after the individual rogue hacker, who is better prosecuted by the Singapore Police and Attorney-General's Chambers.

21 The CMA and the PDPA are meant to address different issues although that could result in an individual/organisation being liable under both pieces of legislation at the same time. The PDPA has anticipated such possibility and has neatly dealt with it under s 50(3)(*d*) of the PDPA.[53]

## IV. Conclusion

22 From the above analysis, Singapore is in a prime position to prevent serious cybersecurity or data protection threats and incidents, and to reduce

50 Revised on 27 July 2017.

51 See ss 13 and 20 of the Personal Data Protection Act 2012 (Act 26 of 2012).

52 See *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319.

53 See also s 4(6) of the Personal Data Protection Act 2012 (Act 26 of 2012).

the risk of abuse of personal data or data that have been obtained via unauthorised or illegal means. The different laws governing cybersecurity, personal data and computer misuse have been carefully calibrated and deliberated to ensure that all risks relating to Singapore's pursuit to be a smart nation, digital economy and global data hub will be minimised. While doing so, the various laws were also crafted in a way to avoid overlapping of jurisdictions or to address that situation when it happens. This obviates the unnecessary duplication of two authorities investigating the same breach whereby only one can take action. To sum up, Singapore has put in place effective laws that keep up with the advancement of technology but not at the unnecessary expense of expanding resources to safeguard the various risk prone areas.

# MONOPOLY RIGHTS VS FREEDOM OF ACCESS: THE COPYRIGHT BALANCE IN A DATA-DRIVEN ECONOMY*

**Trina HA**†
*LLB (Hons) (National University of Singapore)*

**Gavin FOO**‡
*LLB (Hons) (National University of Singapore)*

## I. Introduction

1 In February 2017, the Committee on the Future Economy ("CFE") published its recommendations to guide Singapore's economic strategies for the next decade and achieve an average of 2–3% per year growth for Singapore.[1] The harnessing of data as an asset to generate value was highlighted as an increasingly important source of comparative advantage,[2] with the CFE urging data-driven innovation.[3] This is in line with the increasing worldwide recognition of the potential of data to generate significant financial value and become a key basis of competition, underpinning new waves of productivity growth and innovation.[4]

---

* 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, Legal Department and Head, IP Management (Gov), Intellectual Property Office of Singapore.

‡ Legal Counsel, Legal Department, Intellectual Property Office of Singapore.

1 Report of the Committee on the Future Economy (February 2017) at p 1.

2 Report of the Committee on the Future Economy (February 2017) at paras 37 and 112.

3 Report of the Committee on the Future Economy (February 2017) at paras 111–112.

4 McKinsey Global Institute, *Big Data: The Next Frontier for Innovation, Competition and Productivity* (2011) Executive Summary <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation> (accessed 25 February 2018).

2 In the same year, the Court of Appeal dismissed all but the entirety of an appeal filed by telephone directory publisher Global Yellow Pages Ltd ("GYP") in respect of its action against its competitor, Promedia Directories Pte Ltd ("Promedia") for infringing the alleged copyright in GYP's telephone directories. The High Court found no infringement and this was upheld by the Court of Appeal on the fundamental basis that data are not copyrightable material, even if they are a "valuable commodity" that represent the fruit of an investment.[5]

3 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd*[6] ("*GYP Case*") exemplifies copyright law's fundamental premises and principles, which have resulted in limited (if any) protection over data and data products, such as data that have been further enhanced, derived or analysed,[7] compilations of data and databases. Such material often lie "at the very edge of copyright protection".[8] As a result, certain jurisdictions have taken the view that a *sui generis* database right is required to safeguard the position of database makers against misappropriation of the fruits of their investment, and in turn, incentivise investments in and exploitation of such compilations.[9] In the absence of such a right in Singapore, do the limits

5 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [22] and [34].

6 [2017] 2 SLR 185.

7 For example, Global Yellow Pages Ltd (hereinafter "GYP") claimed that copyright subsisted in the "enhanced data" in its directories, *ie*, individual business listings after they had been verified, embellished, arranged and classified, see *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [11].

8 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [89].

9 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, see, for example, Recital 39: "Whereas … this Directive seeks to safeguard the position of makers of databases against misappropriation of the results of the financial and professional investment made in obtaining and collection the contents by protecting the whole or substantial parts of a database against certain acts by a user or competitor", and Recital 40: "Whereas the object of this *sui generis* right is to ensure protection of any investment in obtaining, verifying or presenting the contents of a database for the limited duration of the right;

(*continued on next page*)

imposed by copyright law therefore impede the achievement of national aspirations to harness data as an asset and catalyse data-driven innovation?

4 This article posits that conferring stronger protection of data and data products through granting monopolies (whether under copyright law or a *sui generis* regime) may be a blunt tool for achieving data-driven innovation and growth – particularly given the realities and complexities of the present data landscape. Far from being an impediment, the limits set by copyright law may in fact spur innovation and growth in the present landscape. The way forward is not to "stretch"[10] copyright's fundamental premises to accommodate protection of data and data products, but to make principled extensions within the boundaries of copyright orthodoxy – one current example is the copyright exception for text and data mining, which is discussed in the last part of this article. These considerations are symptomatic of a broader, perennial tension that both afflicts and informs much of intellectual property law in general – balancing the goal of providing adequate incentives for continued creation (by conferring monopoly rights on database makers, producers and the like) against the competing goal of ensuring adequate access (to data and data products).[11]

## II. *Global Yellow Pages Ltd v Promedia Directories Pte Ltd*: Elucidating principles of copyright protection

### *A. Brief facts and summary of decision*

5 In the *GYP Case*, GYP (the plaintiff) alleged that its competitor Promedia (the defendant) infringed GYP's copyright in GYP's print telephone directories (the *Business Listings*, the *Yellow Pages Business* and the *Yellow Pages Consumer*) and online telephone directory (the *Internet Yellow Pages*). GYP's copyright had been allegedly infringed by Promedia in the

---

whereas such investment may consist in the deployment of financial resources and/or the expending of time, effort and energy".

10 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [26]. At [35], the Court of Appeal rejected GYP's argument that a lower standard of creativity should be adopted in the case of factual compilations, in comparison to other authors' works.

11 See, *eg*, Tan Tee Jim SC, "New Law for Compilations and Databases in Singapore?" (2012) 24 SAcLJ 745 at para 5.

print, digital (CD-ROM) and/or online telephone directories produced and/or maintained by Promedia. GYP also alleged that its copyright was infringed by Promedia's use and deployment of material from GYP's directories in Promedia's temporary database, including by photocopying or scanning the *Business Listings* onto the database.[12] The High Court found no infringement and GYP appealed.

6 The Court of Appeal essentially found GYP's appeal to be unmeritorious because fundamentally, what Promedia took from GYP were data, which are not copyrightable material.[13]

7 The Court of Appeal did not disturb the High Court's finding that copyright did not subsist in the individual business listings in GYP's directories. The High Court found that copyright did not subsist because the form of expression of the individual listings was unoriginal. The selection or arrangement of information within each listing lacked the minimum level of creativity or intellectual effort necessary to make it an original work. Effort, skill and judgment in collecting, verifying, enhancing and arranging the data were not directed at a particular form of expression. Instead, these were directed at ensuring the accuracy of the underlying facts. In the circumstances, granting copyright would amount to granting an impermissible monopoly over the use of bare facts.[14]

8 The Court of Appeal considered whether copyright subsisted in the following three classes of GYP's works:

> (a) The listings of businesses arranged within each business classification in GYP's directories.
> (b) The listings in the *Business Listings*.
> (c) The "seeds" in GYP's directories, which were fictitious listings designed principally to detect and prove copying.[15] GYP proved that

12 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [2], [3] and [8].

13 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [22].

14 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [18(a)].

15 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [50].

Promedia had copied the data in GYP's directories because these seeds were found in Promedia's digital and online directories.[16]

9 The Court of Appeal found that copyright did not subsist in any of these, save for a very narrow instance where the *Business Listings* in (b) was concerned:[17]

(i) As regards (a), the Court of Appeal agreed with the High Court that copyright cannot subsist in the listings arranged within each classification, because the selection of the contents lacked creativity or was in reality a fact-discovery exercise.[18]

(ii) As regards (b), the Court of Appeal held that the *selection* of the listings of businesses in the *Business Listings* lacked creativity, but the *arrangement* exhibited sufficient creativity, albeit only barely so.[19] Even though the listings were presented in alphabetical order,[20] GYP applied specific sorting rules to the listings that made minor tweaks to the arrangement of the listings within the narrow confines of an alphabetical arrangement.[21] The Court of Appeal took the view that the sorting rules taken together, were neither entirely obvious nor inevitable, and this crossed the creativity threshold but just barely.[22]

(iii) As regards (c), the court observed that the very purpose of the "seeds" was to be copied. The court held that copyright cannot subsist in a seed as it is not a literary work to begin with, and in any event,

16 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [10].

17 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [37].

18 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [38]–[42].

19 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [43].

20 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [2].

21 GYP's sorting rules were expressed in five propositions, which were set out in *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [48].

22 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [43]–[49].

the copying of the seeds did not cause GYP any loss or Promedia any gain.[23]

10 Given that the arrangement of the listings in the *Business Listings* exhibited sufficient creativity but only barely so, the *Business Listings* was found to be "cloaked" with copyright, although the resulting protection was "extremely thin".[24] This meant that infringement would only be established by nothing less than near-wholesale taking of the listings in the *Business Listings*, arranged exactly as they were in the *Business Listings*.[25] This was found to be the case as Promedia had photocopied or scanned the entire *Business Listings* onto its temporary database.[26] Its *modus operandi* was to systematically copy the *Business Listings*, which was a key source of information for its master database.[27]

11 Notwithstanding this, Promedia was not liable for infringement because the Court of Appeal held that its photocopying or scanning of the *Business Listings* into the temporary database amounted to fair dealing within s 35 of the Copyright Act[28] ("Copyright Act").[29] The *GYP Case* is significant for the Court of Appeal's elucidation of the approach to assessing fair dealing under s 35 and application to the specific facts in that case, but this aspect of the decision will not be discussed in this article.

12 The *GYP Case* elucidates the following fundamental copyright principles and their implications for protection of data and data products, which are examined in greater detail below:

---

23 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [52].

24 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [49].

25 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [49].

26 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [71].

27 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [65].

28 Cap 63, 2006 Rev Ed.

29 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [71].

(a) Data *per se* are not copyrightable but a compilation of data is.

(b) Data compilations must be "original", *ie*, data must be selected and/or arranged with sufficient creativity.

(c) Data compilations must have human authors.

(d) Copyright in data compilations is "thin".

### *B. Data* per se *are not copyrightable but a compilation of data is*

13 It is axiomatic that copyright does not protect ideas and facts but the form of expression of such. Correspondingly, data *per se* are not protected; a compilation of data however, may attract copyright. Article 10(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS Agreement") demonstrates the international consensus on this distinction and provides:

> Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.

14 The position under the Copyright Act complies with Art 10(2) of the TRIPS Agreement. The Copyright Act protects a compilation of data as an original literary work, but any copyright subsisting in such a compilation is "limited to the selection or arrangement of its contents which constitutes an intellectual creation"; copyright does not subsist in the underlying data or facts.[30]

15 Examples of compilations of facts and/or data that have been protected by copyright law include tables, databases, telephone directories, street directories, railway tables, examination papers, trade catalogues, a racing information service, football fixtures, betting lists and listings of television broadcast programmes.[31]

---

30 Copyright Act (Cap 63, 2006 Rev Ed) ss 4, 7A and 27. As the Court of Appeal stressed in *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [15]: "Copyright protects not ideas, facts or data, but the expression thereof."

31 Tan Tee Jim SC, "New Law for Compilations and Databases in Singapore?" (2012) 24 SAcLJ 745 at para 12.

16 By protecting only expressions of data and other facts, copyright law ensures that the underlying data and facts always remain in the public domain and free to use.

### *C. Data compilations must be "original",* ie*, data must be selected and/or arranged with sufficient creativity*

17 For copyright to subsist in a compilation of data, the compilation must be "original".[32] There are two main approaches to determine whether a compilation is original. These approaches have differing views on the quality and the object of the effort in producing a work, and were summarised by the Court of Appeal in the *GYP Case* as follows:[33]

> (a) The "sweat of the brow" approach. This considers the author's labour and industry to be relevant, and admits consideration of the effort taken in the preparatory steps leading to the reduction of the work to its final form.
>
> (b) The "creativity" approach. This places emphasis on the end product of the work and considers efforts applied towards the formulation of how that end product will be expressed. This approach does not protect preparatory efforts or the process of gathering facts, and an expression of data that involves little ingenuity or skill beyond mechanical labour or routine programming may well not attract copyright protection.[34]

18 The Court of Appeal observed that there has been a "noticeable retreat from the 'sweat of the brow' approach that once featured in the decisions of the Australian and English courts", and the creativity approach applies in Singapore.[35] For copyright to subsist in any literary work, there must be an

---

32 Copyright Act (Cap 63, 2006 Rev Ed) s 7A read with s 27.

33 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [23].

34 *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* [2011] 4 SLR 381 (CA) at [37].

35 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [26].

"authorial creation that is causally connected with the engagement of the human intellect".[36] This means:[37]

> … the application of intellectual effort, creativity, or the exercise of mental labour, skill or judgment. Effort (even intellectual) that is applied not towards the authorial creation but towards other ends such as the verification of facts will not be relevant … even if such verified facts might be the eventual subject of the authorial creation … It follows from this that the compiler must exercise sufficient creativity in selecting or arranging the material within the compilation; and if the compiler does so, the resulting copyright will only protect the original expression in the form of the selection or arrangement of the material, as the case may be …

19 There is no prescribed minimum level of creativity required for copyright to subsist in a compilation.[38] Instead, the sufficiency of creativity is a question of fact and degree, *ie*, whether in each case the human acts done and choices made in reducing the universe of raw information and data into a compilation demonstrate sufficient creativity and bear sufficient causal nexus with the final work (*ie*, the compilation) such that the compilation is found to be "original" for the purpose of copyright subsistence.[39]

20 This exercise is heavily fact-centric and can be a "nuanced" one, as the Court of Appeal acknowledged in the *GYP Case*.[40] At one end of the spectrum, there are managerial decisions which clearly do not merit copyright protection – such as whether to publish or update a phone directory. Then there are purely mechanical tasks that, taken alone, would not cross the creativity threshold – such as the algorithmic collection or arrangement of data. Then there are choices in between that require human judgment and do impact the selection or arrangement of the material, and

36 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [24].

37 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [24].

38 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [28].

39 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [28]–[30].

40 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [30]–[31].

which might more properly be regarded as authorial in nature.[41] In essence, the spark of creativity must extend beyond mere data aggregation and input.

### *D. Data compilations must have human authors*

21 For copyright to subsist in a compilation of data, the author of the compilation must also be a natural person (as opposed to a non-living "person" such as an incorporated body) who must first be identified. Otherwise, the work product cannot be deemed original for the purpose of copyright subsistence.[42] This principle was alluded to although not expressly discussed in the *GYP Case*.[43] The principle was the subject of a different Court of Appeal decision in *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd*[44] ("*APP Case*"), where the court held that it is not necessary to name each and every human author to make out a claim for copyright protection but it has to be shown that the work product in question has been generated from human author(s) working alone or collaboratively, *ie*, the existence of such persons must be clearly established.[45]

22 This principle has potentially wide-ranging implications given that "most of the produced and collected data in the digital economy, which are

41 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [28].

42 *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* [2011] 4 SLR 381 at [75].

43 See, *eg*, *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [24]: "for copyright to subsist in any literary work, there must be authorial creation that is causally connected with the engagement of the human intellect", and [28]: "the sufficiency of intellectual effort will often be … a question of 'fact and degree' … What is common across the jurisdictions, however, is that each court seeks to characterise the human acts done and decisions made in reducing the universe of raw information into a work".

44 [2011] 4 SLR 381.

45 *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* [2011] 4 SLR 381 at [75].

so important for data analytics … are machine-generated data".[46] Further, large corporations that invest significant labour and financial resources to produce compilations often employ a high degree of automation and an army of workers in the entire production chain whose contribution lies in merely executing discrete tasks of data gathering, data verification, data entry and data presentation. It is not unusual for different steps in the production of these compilations to be outsourced or allocated to subcontractors or employees located in different countries. Even if the names of these individuals may be identified, it is unlikely that the human author requirement – which possesses the aforesaid element of creativity – would be satisfied.[47]

23 To the extent that data compilations do not satisfy the human author requirement, copyright will not subsist in the same. Both this requirement and the creativity approach acknowledge the significant role of technology in producing compilation works and promote an important societal goal of ensuring public access to knowledge contained in data compilations.[48] Such material will be entirely free to access by other players in the data landscape, and this may then spur innovation and new business models.

### *E. "Thin" copyright in data compilations*

24 The foregoing principles relate to copyright subsistence, *ie*, if a compilation of data is original and authored by human author(s), it would conceivably be eligible for copyright protection. However, even if copyright subsists, the protection conferred would be "thin". The thinner the protection, the more substantial the copying must be before a finding of

46 Wolfgang Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis* at p 2 <https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf> (accessed 14 February 2018).

47 David Tan, "Copyright in Compilations: Embarking on a Renewed Quest for the Human Author and the Creative Spark" (2013) 18 *Media and Arts Law Review* 151 at 160–161.

48 David Tan, "Copyright in Compilations: Embarking on a Renewed Quest for the Human Author and the Creative Spark" (2013) 18 *Media and Arts Law Review* 151 at 162.

copyright infringement will be made. The Court of Appeal's explanation in the *GYP Case* is worth setting out in full:[49]

> [T]he method of analysis is heavily shaped by what it is in a work that attracts copyright protection, especially where infringement and fair dealing are concerned. In other words, there is a nexus between the originality, skill and effort that goes into a work, and the substantiality of copying required to establish infringement. Thus, ***although copyright may subsist in a work*** *as a whole,* ***there would be no infringement of such copyright unless one copies the work as a whole, or a substantial portion of the part of the work*** *that attracts copyright protection in the first place* … For example, the copyright that subsists in a *compilation of all the news articles* published by a certain agency in a certain month by virtue only of its *thematic arrangement* would not be infringed by another compilation of the same selection of articles arranged *chronologically* because, even though the same underlying material might have been copied, the arrangement, *in which copyright was found to subsist*, was not … ***the thinner the copyright protection, the more substantial the copying must be before a finding of infringement will be made.***[emphasis in bold italics added; emphasis in italics in original]

## III. Reappraising the case for conferring stronger monopolies in data and data products

### *A. Sui generis right(s) in data and data products*

25 As can be seen from the above principles, copyright law tends to lean in favour of allowing freedom of access to and use of data and data products. In the *GYP Case*, the Court of Appeal explained that "the commercial immorality underlying … conduct [involving appropriation of data or facts that represents the fruit of an investment] … is … not within the purview of copyright law … [and] is more properly the province of a *sui generis* database right, which has been recognised in the European Union but not in Singapore".[50] Based on an incentive theory of intellectual property, the limited protection of data and data products under copyright law and lack of a *sui generis* database right may suggest that there is or will

49 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [16].

50 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [34].

be a lack of incentive to invest in and monetise data and data products, which in turn, will impede innovation in Singapore. The logic is that if subsequent compilers can take data from a compilation with impunity, and are thereby able to sell competing compilations at a lower price, there would be little incentive to invest in the creation of factual compilations in unchartered areas.[51] Any advantages of lead time may be diminished in an industry where the buying public would be attracted to the later compilations because they are usually an updated version.[52]

26 Such reasoning underpinned the introduction of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases ("EU Database Directive), which gives the maker of a database who shows that there has been qualitatively and/or quantitatively a substantial investment in obtaining, verifying or presenting the contents of the database, a right to prevent extraction and/or re-utilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.[53]

27 Already, there are calls in the European Union ("EU") to go beyond the EU Database Directive and create a "new data producer right with the objective of enhancing the tradability of non-personal or anonymised machine-generated data as an economic good".[54] It is hoped that this would

---

51 Ng-Loy Wee Loon, "Copyright Protection for Traditional Compilations of Fact and Computerized Databases – Is Sweat Copyrightable?" [1995] Sing JLS 96 at 117.

52 Ng-Loy Wee Loon, "Copyright Protection for Traditional Compilations of Fact and Computerized Databases – Is Sweat Copyrightable?" [1995] Sing JLS 96 at 117.

53 Article 7(1) of the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. "Database" is defined in Art 1(2) as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means", and "maker of a database" is defined in Recital 41 as the "person who takes the initiative and the risk of investing … [and] excludes subcontractors".

54 Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication "Building a European Data Economy" (SWD/2017/02 final) at p 33 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0002> (accessed 14 February 2018).

facilitate and incentivise sharing of such data and protect investments and assets.[55] The proposal is in its preliminary stages. At the time of writing, the right has been envisaged as either a right *in rem* (*ie*, a property right enforceable against the world independent of contractual relations, which would mean a right to utilise the data and license its usage) or a set of purely defensive rights providing for the capacity to sue for misappropriation of data (similar to an action for breach of confidence).[56]

### *B. Are monopolies in data and data products desirable or even appropriate?*

28 Whether the introduction of such *sui generis* right(s) is the way to go for Singapore is a matter requiring careful consideration. For the present purpose, it suffices to observe that the appeal of the incentive theory (*ie*, lack of protection kills creativity) lies in the simplicity of its logic, which may not always hold true. In 2016, an economic study assessing the need for a new intellectual property right on data in the EU directly challenged the incentive theory:[57]

> In the discussion about data property so far, nobody has claimed that we have a general incentive problem in the digital economy as regards the collection, production, and analysis of data. To the contrary, the empirical fact of the massive and often simple production of huge amounts of data and their analysis seems to be one of the most important characteristics of Big Data and the digital economy. The amount of collected data is increasing exponentially, and it is widely expected that through the spreading of sensor technology and the 'internet of things' this trend will continue for the foreseeable future.

---

55 Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication "Building a European Data Economy" (SWD/2017/02 final) at p 30.

56 Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication "Building a European Data Economy" (SWD/2017/02 final) at pp 33–34.

57 Wolfgang Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis* at pp 8–9 <https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf> (accessed 14 February 2018).

29 It may even be said that in the world of databases, *copying actually sparks innovation*. The US, where copying is allowed in the absence of a *sui generis* database right, has a much more vibrant database industry than Europe. In particular, as a result of the higher originality standard for compilation works in the US, the cost of creating new and better databases has been reduced. The European approach may have resulted in higher profits for individual database producers but it has not grown the overall industry, in part because it "chokes off the kind of beneficial tweaking and reworking that are so useful to innovation".[58]

30 It should therefore be considered whether the grant of monopolies in data and data products sits well with the "functional logic" of Big Data and the digital economy in the first place – to use data from many different sources, combine them, analyse them, derive new data, which again can be used for further analyses in combination with other data.[59] One of the characteristics of the data economy is that data can often be used for analyses in many different contexts and for solving many different problems. It has thus been claimed that in order to develop innovations in the digital economy, it is essential to have easy access to many different kinds of data and that all impediments to the free flow of data should be eliminated as far as possible.[60]

31 Ultimately, the complexity of the contemporary data landscape should not be overlooked – whether in terms of the players in the landscape and relationship between one another;[61] the range and nature of dealings with

---

58 David Tan, "Copyright in compilations: Embarking on a renewed quest for the human author and the creative spark" (2013) 18 *Media and Arts Law Review* 151 at 162–163.

59 Wolfgang Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis* at p 19 <https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf> (accessed 14 February 2018).

60 Wolfgang Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis* at p 19 <https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf> (accessed 14 February 2018).

61 In a study of the data landscape in Singapore conducted by KPMG Services Pte Ltd and commissioned by the Competition Commission of Singapore, the main players in the Singapore data landscape were identified as government

(*continued on next page*)

data and data products; or the benefits accompanying such dealings.[62] This includes the emergence of "complex new value networks of firms", where connected firms often contribute technically and economically to the production and processing of data. These complexities do not admit clear answers as to who should be granted monopoly rights and reap the economic value of data and data products: The data producer? The firm that is economically responsible for producing the data? The firm that can use the data most efficiently? Or the firm that can benefit the most from the data?[63] The very notion of monopoly rights may not be appropriate in these circumstances.

## IV. Copyright exception for text and data mining

32 As a result of the increasing prominence and proliferation of data and data products, there is a burgeoning chorus of views that text and data

---

agencies, businesses, customers, data analytics solutions providers, data storage providers, and data aggregators and brokers, see *Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights* (16 August 2017) at paras 27–42 <https://www.ccs.gov.sg/media-and-publications/publications/studies-research-papers/occasional-papers/data-engine-for-growth> (accessed 14 February 2018).

62 For example, it has been suggested that the data economy measures the overall impact of the data market on the economy as a whole, and involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery and exploitation of data enabled by digital technologies. This includes not only the direct effects of the data market on the economy, but also the indirect and induced effects. The benefits extend beyond direct monetisation of data and data products, and can also translate into revenue increases, cost optimisation, operational efficiency, operational effectiveness and promotion of information and communication technology ("ICT") adoption, entrepreneurship and new venture; see *Final Results of the European Data Market Study Measuring the Size and Trends of the EU Data Economy, Executive Summary* (1 February 2017) at pp 10 and 20–21 <https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy> (accessed 25 February 2018).

63 Wolfgang Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis* at pp 6 and 15 <https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf> (accessed 14 February 2018).

mining activities – which both create and use data and data products – should be conducted without risk of copyright infringement. Legitimising text and data mining activities is consistent with orthodox copyright principles, and as an alternative to granting monopolies in data and data products, may even achieve greater innovation and growth in the contemporary data-driven economy.

33 "Text and data mining" generally refers to the use of automated analytical techniques to analyse text and data in digital form in order to generate information and insights such as patterns, trends and correlations.[64] Such information and insights may not have been possible or feasible to obtain through manual effort. These techniques work by deriving information from machine-read material – copying large quantities of material, extracting the data, and thereafter analysing the data.[65] The actual process of analysis may involve making further copies of the material, including by storage in computers or on any medium by electronic means.

34 To the extent that such techniques involve copying or reproducing material that may be protected by copyright, text and data mining activities may give rise to liability for copyright infringement in the absence of a specific copyright exception. This can represent a barrier to innovation and economic opportunity – an independent review of intellectual property and growth in the UK in 2011 found that research scientists, including medical researchers, were being hampered from using computerised search and analysis techniques on data and text because the then-copyright law in the UK could possibly forbid or restrict such usage.[66]

---

64 See, for example, the definitions of "text and data mining" in Art 2(2) of the Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market <https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market> (accessed 15 February 2018); and Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at para 11.57.

65 (Hargreaves review) Supporting Document T – Text Mining and Data Analytics in *Call for Evidence* Responses at p 1 <http://webarchive.nationalarchives.gov.uk/20140603125140/http://www.ipo.gov.uk/ipreview-doc-t.pdf> (accessed 15 February 2018).

66 Ian Hargreaves, *Digital Opportunity: A Review of Intellectual Property and Growth* (May 2011) at para 5.10.

35 Given this, copyright legislation in the UK[67] and Japan[68] provide for a specific copyright exception for text and data mining. The exception has been proposed in Singapore,[69] as well as other jurisdictions such as Australia[70] and the EU.[71]

36 The exception is supported by "growing recognition" that text and data mining should not be infringement because it is "non-expressive use".[72] Non-expressive use leans on the fundamental principle that copyright law protects only the expression of facts, ideas and data. This point is aptly illustrated by the following example from the Australian Law Reform Commission:[73]

> Consider a computer algorithm employed to search through a text to obtain metadata, which discovers two facts about Moby Dick:
>
> > first, that the word "whale" appears 1119 times; second, that the word "dinosaur" appears 0 times. While a whale is certainly central to the expression contained in Moby Dick, this data is not. Rather, metadata of this sort … is factual and non-expressive, and incapable of infringing the rights of copyright holders.

37 In other words, the text and data mining exception dovetails with the classic limits of copyright law. The fact-discovery purposes enabled by text and data mining should be permitted because such techniques do not seek

---

67 Copyright, Designs and Patents Act 1988 (c 48) (UK) s 29A ("Copies for text and data analysis for non-commercial research").

68 Japan Copyright Law Arti 47*septies* ("Reproduction, *etc* for information analysis").

69 MinLaw and IPOS Public Consultation on Proposed Changes to Singapore's Copyright Regime (23 August 2016), Proposal 9 at paras 3.61–3.64.

70 Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at paras 11.57–11.84.

71 Article 3 of the Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market <https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market> (accessed 15 February 2018).

72 Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at para 11.60.

73 Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at para 11.60, citing M Jockers, M Sag & J Schultz, *Brief of Digital Humanities and Law Scholars as Amici Curiae in Authors Guild v Hathitrust* (2013) at p 18.

to make use of the expressions that are intended for copyright protection.[74] Uses that treat copyright works as mere data – rather than for their expressive value – do not compete with the original works and should not be treated as falling within the scope of the copyright owner's rights.[75] As Professor Ian Hargreaves explained:[76]

> [Text and data mining] do[es] not directly trade on the underlying creative and expressive purpose of [copyright] work[s] … This is not about overriding the aim of copyright – these uses do not compete with the normal exploitation of the work itself – indeed, they may facilitate it … That these new uses happen to fall within the scope of copyright regulation is essentially a side effect of how copyright has been defined, rather than being directly relevant to what copyright is supposed to protect [*ie*, expressions].

38 The text and data mining exception may also be understood as an extension of the specific fair dealing exception for research (*eg*, the UK[77] and Australia[78]) or a subset of fair use/general fair dealing (*eg*, the US[79] and Singapore[80]). To the extent that the author's original expression is not

---

74 See also, (Hargreaves review) Supporting Document T – Text Mining and Data Analytics in *Call for Evidence* Responses at p 1 <http://webarchive.nationalarchives.gov.uk/20140603125140/http://www.ipo.gov.uk/ipreview-doc-t.pdf> (accessed 15 February 2018): "There are strong arguments for amending the legal framework to provide a mechanism to allow for text and data mining to be undertaken without requiring permission from rights holders because the technique does not seek to make use of the expressions intended for protection."

75 Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at para 11.62.

76 Ian Hargreaves, *Digital Opportunity: A Review of Intellectual Property and Growth* (May 2011) at para 5.24.

77 Copyright, Designs and Patents Act 1988 (c 48) (UK) ss 29 and 29A.

78 Australia Copyright Act 1968 s 40.

79 US Copyright Act 17 USC §107. For an analysis of how text and data mining may be understood as fair use within the meaning of §107, see Krista L Cox, "Research Libraries and New Technologies, Promoting Access to Information, Learning, and Innovation for Today and the Future" (2016) 13:1 I/S: J L & Pol'y for Info Soc'y 261 at 266–269.

80 Copyright Act (Cap 63, 2006 Rev Ed) ss 35 and 109. In *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185, the Court of Appeal found that Promedia's photocopying or scanning of the *Business Listings* into its temporary database amounted to fair dealing within s 35. The court's

(*continued on next page*)

substituted, non-expressive uses in the form of text and data mining may be considered highly transformative: their "purpose and character" is such that they do not merely supersede the objects of the original creation.[81]

39 Copyright orthodoxy aside, the text and data mining exception is aligned with the "functional logic" of Big Data and the digital economy.[82] At a commercial level, the ability to extract value is an increasingly important feature of the digital economy. Tellingly, there is "widespread acknowledgment" that text and data mining can benefit the research community and in doing so, encourage innovation;[83] it paves the way for novel discoveries, increased research output, early identification of problems,[84] and has the potential to grant "immense inferential power" to allow businesses, researchers and institutions to make proactive, knowledge-driven decisions.[85] Businesses can better understand and predict customers' interests, focus efforts and resources on more profitable areas, and achieve better performance overall.[86] Text and data mining has also been known to increase the speed of processes and reduce transaction costs across a range of applications.[87]

40 To reap such benefits and more, a text and data mining exception has been proposed as part of a comprehensive review of Singapore's copyright

---

reasoning suggests that Promedia only made non-expressive use of the Business Listings (at [87]–[91]).

81 Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at para 11.61.

82 See para 30 above.

83 Recital 8 of the Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market <https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market> (accessed 15 February 2018).

84 Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at para 11.58.

85 Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at para 11.59.

86 Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, November 2013) at para 11.59.

87 (Hargreaves review) Supporting Document T – Text Mining and Data Analytics in *Call for Evidence* Responses at p 5 <http://webarchive.nationalarchives.gov.uk/20140603125140/http://www.ipo.gov.uk/ipreview-doc-t.pdf> (accessed 15 February 2018).

regime.[88] The public consultation paper explained that text and data mining is "integral to Singapore's Smart Nation initiative and allowing for such activities to operate freely would … help to create and disseminate knowledge."[89] The *Report of the Committee on the Future Economy*[90] similarly suggests that the exception assumes a strategic, national significance, as the CFE had advocated the use of data analytics to develop innovative solutions that serve the needs of and solve specific problems within various industries in Singapore.[91]

41 The proposed exception in Singapore will allow copying or reproduction of copyright works for the purpose of data analysis. Users of such works must have legitimate access to the works in the first place (such as through paid subscriptions or access that is not limited by any arrangement where content is accessible only after payment). While both commercial and non-commercial activities would be permitted under the proposed exception, the copying and reproduction must be for the purpose of data analysis to benefit from the exception; the exception is not intended to cover situations where the commercial benefit comes from the actual copies of the copyright works, instead of the data analysis.[92]

## V. Concluding remarks

42 The intrinsic balance in copyright law is aptly summed up by the Court of Appeal in the *GYP Case*:[93]

88 MinLaw and IPOS Public Consultation on Proposed Changes to Singapore's Copyright Regime (23 August 2016), Proposal 9 at paras 3.61–3.64.

89 MinLaw and IPOS Public Consultation on Proposed Changes to Singapore's Copyright Regime (23 August 2016), Proposal 9 at paras 3.63.

90 February 2017.

91 Report of the Committee on the Future Economy (February 2017) at para 109a.

92 As proposed in para 3.64 of the MinLaw and IPOS Public Consultation on Proposed Changes to Singapore's Copyright Regime (23 August 2016). Whether such an exception will be created, and if so, the details of the exception, is subject to the Government's eventual recommendations taking into account stakeholder feedback from the consultation.

93 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [74].

> Copyright law is meant to promote creativity and innovation by granting exclusive rights to copyright holders, but there is equally a public interest in not allowing copyright law to hinder creativity and innovation.

43 Where data and data products are concerned, the balance in copyright law tends to lean in favour of allowing free access and use, given the fact-based nature of such material and high degree of automation often involved in its creation. A text and data mining exception may tilt the balance yet further towards allowing uninhibited access and use. Such developments would spur data-driven innovation and growth.

44 Of course, it is not a zero-sum game in that there is always a possibility that *sui generis* right(s) in data and data products can complement copyright law to achieve greater innovation overall. One should also consider other measures of protecting data and data products, such as the law of contract as observed in the *GYP Case*,[94] and depending on the circumstances, the law of confidence and use of technological protection measures.[95] Such discussions are, however, beyond the scope of this article. Nevertheless, like obsolete technologies, the case for granting monopolies in data and data products should be reappraised in the light of the realities and complexities of the contemporary data landscape.

---

94 *Global Yellow Pages Ltd v Promedia Directories Pte Ltd* [2017] 2 SLR 185 at [35] (citing the observations of *amicus curiae* Professor David Llewelyn).

95 For a discussion on these other modes of protection, see, for example, Tan Tee Jim SC, "New Law for Compilations and Databases in Singapore?" (2012) 24 SAcLJ 745 at paras 113–123.

# PERSONAL DATA AND CUSTOMER INFORMATION IN THE AGE OF FINTECH*

**Alexander YAP Wei-Ming**†
*MA (Oxon); Advocate and Solicitor (Singapore)*

**Adrian ANG**‡
*MA (Oxon); Advocate and Solicitor (Singapore)*

**Claudice WEE Li Yun**§
*LLB (University of London); Advocate and Solicitor (Singapore)*

## I. Introduction

1 Today, one would be hard-pressed to find an individual who has not come across the ubiquitous "FinTech" buzzword or enjoyed the benefit of products introduced by participants in the growing FinTech industry. The pervasiveness of technology has brought the portmanteau into the global limelight, as financial services become more technologically-enabled, and customers enjoy greater convenience, increased accessibility and tailor-made user experiences.

2 That being said, the benefits of merging the financial sector with technology come at a price. While banks and other financial institutions are familiar with the scope and requirements of financial regulation, start-ups and companies with a "technology" background are sometimes surprised by the degree to which they are subject to new (to them) regulatory requirements and scrutiny from sectoral regulators; although this should be

---

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

† Partner, Allen & Gledhill LLP. Alexander graduated from Keble College, University of Oxford. Adrian and Alexander are the co-heads of Allen & Gledhill LLP's FinTech practice.

‡ Partner, Allen & Gledhill LLP. Adrian graduated from Merton College, University of Oxford.

§ Associate, Allen & Gledhill LLP. Claudice graduated from King's College London, University of London.

expected as the regulators simply want to ensure that existing protections and legal frameworks are not circumvented by, or through, innovation. Given that personal data are now regarded as being representative of an emerging asset class potentially every bit as valuable as gold or oil,[1] a major concern of consumers and industry players alike is the protection of personal customer data.

3 Are all FinTech industry participants subject to the data protection requirements under both the Singapore financial regulatory regime and the overarching data protection regime established under the Personal Data Protection Act 2012[2] ("PDPA")? At first blush, s 4(6) of the PDPA, and in particular s 4(6)(*b*), appears to suggest that the requirements under the PDPA are to be regarded as secondary to "the provisions of other written law",[3] which includes the requirements under the financial regulatory regime such as s 47 of the Banking Act.[4] However, on closer inspection, the carve out in s 4(6) of the PDPA will only apply in the limited instance where a specific requirement under Pts III to VI of the PDPA ("Data Protection Provisions") is "inconsistent" with the provisions of any other written law in some way, and there is limited guidance which squarely addresses when a provision of other written law will be regarded to be "inconsistent" with any of the Data Protection Provisions as to invoke s 4(6) of the PDPA.

4 The remainder of this article will examine the interplay between the Singapore financial regulatory regime and the data protection regime established under the PDPA, discuss several instances in which provisions under the financial regulatory regime may potentially be inconsistent with the Data Protection Provisions so as to trigger the exception under s 4(6) of the PDPA, and highlight practical approaches which FinTech industry

1 World Economic Forum, "Personal Data: The Emergence of a New Asset Class" (2011) at p 7, see also World Economic Forum, "Will the Future Be Human?" (Yuval Harari) (2018).

2 Act 26 of 2012.

3 Section 2(1) of the Interpretation Act (Cap 1, 2002 Rev Ed) defines "written law" as "the Constitution and all previous Constitutions having application to Singapore and all Acts, Ordinances and enactments by whatever name called and subsidiary legislation made thereunder for the time being in force in Singapore".

4 Cap 19, 2008 Rev Ed.

participants (including established financial institutions such as banks and certain capital markets services licence holders) may wish to consider. The article will conclude by touching briefly on more general practical measures which organisations (including FinTech industry participants) may wish to consider (in addition to prescribed obligations under specific legislation) when collecting, using, disclosing or otherwise processing personal data.[5]

## II. Balance between regulation and innovation

5 While on the one hand, incumbent financial institutions and other more established players in the FinTech industry have become accustomed to the rigours of compliance and the requirements which arise from scrutiny by regulators,[6] start-ups and other new entrants, especially those struggling with funding or liquidity, may not prioritise compliance with the various rigorous regulatory regimes.

6 Sectoral regulators, including the Personal Data Protection Commission ("PDPC") and the Monetary Authority of Singapore ("MAS"), are aware of this and have taken various steps to avoid stifling innovation in the burgeoning FinTech industry in Singapore, with one notable initiative being the introduction of various regulatory sandboxes.[7]

---

5 The Personal Data Protection Commission in a written response to feedback, issued on 1 February 2018, indicated that it intends to provide for "Legitimate Interests" as a basis to collect, use or disclose personal data regardless of consent. Depending on the manner in which such new basis of collection, use and disclosure of personal data is permitted within the Singapore data protection regime, this could be beneficial for FinTech industry participants who are not in a position to directly or indirectly obtain consent from individuals, especially those participants whose products or services are targeted towards protecting legitimate interests that will have economic, social, security or other benefits for the public (or a section thereof), such as credit card or online payment fraud detection solutions.

6 Deloitte, "Singapore FinTech Festival 2017: FinTech's Place in the Sun" (2017).

7 The Monetary Authority of Singapore's FinTech Regulatory Sandbox is described at <http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox.aspx> (accessed 30 March 2018); the Personal Data Protection Commission's data sharing arrangements regulatory sandbox is described at <https://www.pdpc.gov.sg/Legislation-and-

(*continued on next page*)

## III. Crossovers in regulatory regimes: Inconsistencies or overlaps?

7 Prior to the introduction of the PDPA, the regulatory framework for the protection of personal information was fragmented and patchwork in terms of coverage, with a multitude of different statutes and regulations each touching upon secrecy and disclosure or obligations of confidentiality to a certain, but ultimately limited, extent.[8] This patchwork protection, while largely intact, has now been overshadowed by the overarching framework of protection for personal data introduced by the PDPA. As a result, there are numerous crossovers or interactions between the provisions of the PDPA and the provisions of other written laws ranging from the Telecommunications Act[9] to the Private Hospitals and Medical Clinics Regulations.[10] However, this article is focused on a few specific crossovers which are more pertinent in the context of FinTech.

### *A. MAS Notice 626 on the Prevention of Money Laundering and Countering the Financing of Terrorism – Banks*

8 MAS Notice 626 on the Prevention of Money Laundering and Countering the Financing of Terrorism – Banks ("MAS Notice 626") applies to banks in Singapore and sets out certain obligations that such banks will need to comply with in the field of anti-money laundering and countering the financing of terrorism. Looking at MAS Notice 626,[11] a convincing argument may be made for the existence of a relatively uncontentious inconsistency between para 13.4 of MAS Notice 626 and the Data Protection Provisions such that s 4(6) of the PDPA will be invoked. Paragraph 13.4 of MAS Notice 626 provides that:

---

Guidelines/Exemption-Requests/Data-Sharing-Arrangements> (accessed 30 March 2018).

8 Vili Lehdonvirta, "European Union Data Protection Directive: Adequacy of Data Protection in Singapore" [2004] Sing JLS 511.

9 Cap 323, 2000 Rev Ed.

10 Cap 248, Rg 1, 2002 Rev Ed.

11 A similar analysis may be applied to other notices issued by the Monetary Authority of Singapore to financial institutions on anti-money laundering and countering the financing of terrorism, pursuant to the Monetary Authority of Singapore Act (Cap 186, 1999 Rev Ed).

> [F]or the purposes of complying with the Notice, a bank may, whether directly or through a third party, *collect, use, and disclose personal data* of an individual customer, an individual appointed to act on behalf of a customer, an individual connected party of a customer or an individual beneficial owner of a customer, *without the respective individual's consent*. [emphasis added]

9 On a plain reading of the language of para 13.4, the direct inconsistency between para 13.4 and the requirement under the PDPA that organisations may only collect, use or disclose personal data about an individual with that individual's consent[12] is clear. As such, it is the view of the authors that where a bank is obliged under MAS Notice 626 to make a disclosure of information which may comprise personal data, the bank will be able to rely on the exception in s 4(6) of the PDPA in order to comply with such request and give effect to such disclosure, notwithstanding the fact that the bank may not have obtained consent from the relevant individual(s) for such disclosure of their personal data.

10 That being said, banks ought to be mindful that s 4(6) of the PDPA may only be relied on in so far as the inconsistency persists, and is not intended to operate as, nor should it be used as, a carte blanche to flout the protections established by the PDPA. For example, while it is arguable that s 4(6) of the PDPA will operate to allow the disclosure of personal data pursuant to the operation of MAS Notice 626, where the recipient is located outside of Singapore the organisation should continue to ensure that the transfer to such recipient is carried out in a manner compliant with s 26 of the PDPA, given that the transfer limitation obligation is a separate Data Protection Provision which refers specifically to transfers rather than collection, use or disclosure, and is accordingly not inconsistent with MAS Notice 626.

### *B. Banking secrecy obligations under section 47 of Banking Act*

11 Banking secrecy in Singapore is regulated under s 47 of the Banking Act, which states that customer information shall not, in any way, be disclosed by a bank in Singapore or any of its officers to any other person except for such purposes and to such persons as are specified in the Third Schedule to the Banking Act (subject to the conditions specified therein).

12 Personal Data Protection Act 2012 (Act 26 of 2012) s 13.

Given the substantial overlap in the definition of "customer information"[13] and "personal data",[14] there is an argument to be made that s 4(6) of the PDPA may be invoked in so far as any of the Data Protection Provisions are inconsistent with a provision in the Third Schedule to the Banking Act.

12 That being said, the authors are of the view that not all of the exceptions under the Third Schedule to the Banking Act are inconsistent with those of the PDPA. Taking para 1 of Pt I of the Third Schedule to the Banking Act as an example, disclosure is not prohibited where the purpose for the disclosure is "*permitted in writing* by the customer or, if he is deceased, his appointed personal representative" [emphasis added]. In the light of the foregoing, it would stand to reason that a bank would need to determine the scope of the written consent it is seeking from the customer (or his appointed personal representative) and notify such individual and obtain his consent. In this manner, there is strictly speaking no inconsistency between this approach and the obligation to notify individuals of the purposes for which the bank will be collecting, using and disclosing personal data and thereafter obtaining consent from such individuals for such collection, use and disclosure under the PDPA. As such, practically speaking, it would appear that in order for a bank to disclose customer information which also happens to include personal data, the bank will need to comply with:

(a) the banking secrecy regime by relying on an exception under the Third Schedule to the Banking Act; and

(b) the PDPA, by obtaining consent, express or deemed, or otherwise relying on a valid exception under the PDPA regime.

---

13 "Customer information" is defined under s 40A of the Banking Act (Cap 19, 2008 Rev Ed) to mean: "(*a*) any information relating to, or any particulars of, an account of a customer of the bank, whether the account is in respect of a loan, investment or any other type of transaction, but does not include any information that is not referable to any named customer or group of named customers; or (*b*) deposit information".

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

### *C. Trust secrecy obligations under section 49 of Trust Companies Act*

13 A parallel concept to the interplay between the banking secrecy regime and the PDPA regime may be found in respect of the trust secrecy obligations under s 49 of the Trust Companies Act,[15] which provides that information regarding a protected party or the business or other affairs of the protected party shall not, in any way, be disclosed by a licensed trust company in Singapore or any of its officers to any other person except for such purposes and to such persons as are specified in the Third Schedule to the Trust Companies Act. Taking a similar example, para 1 of Pt I of the Third Schedule to the Trust Companies Act states that information may be disclosed where "*permitted in writing* by a settlor or a protected party about whom the information regards, or if he is deceased, his appointed personal representative" [emphasis added]. As such, the reasoning set out above[16] applies in the same manner such that practically speaking, in order for a trust company to disclose information which also happens to include personal data, the trust company will need to comply with:

(a) the trust secrecy regime by relying on an exception under the Third Schedule to the Trust Companies Act; and

(b) the PDPA, by obtaining consent, express or deemed, or otherwise relying on a valid exception under the PDPA regime.

### *D. Regulation 47(2) of Securities and Futures (Licensing and Conduct of Business) Regulations*

14 One final example of a crossover presents itself in reg 47(2) of the Securities and Futures (Licensing and Conduct of Business) Regulations,[17] which restricts holders of a capital markets services licence to deal in securities, trade in futures contract or carry out leveraged foreign exchange trading, or the representative of such a holder, from divulging information relating to a customer's order held by it, unless the disclosure:

15 Cap 336, 2006 Rev Ed.

16 See para 12 above.

17 Cap 289, Rg 10, 2004 Rev Ed.

(a) is necessary for the effective execution of the order;

(b) is permitted under the rules of the relevant securities exchange, futures exchange, clearing house or recognised trading system provider, as the case may be; or

(c) is required by the MAS under the Securities and Futures Act[18] or the Securities and Futures (Licensing and Conduct of Business) Regulations.

15 However, again, the provisions of reg 47(2) do not appear to be inherently inconsistent with the regulatory regime under the PDPA. To elaborate, the obligation under reg 47(2) is phrased as a restriction prohibiting disclosures of information relating to a customer's order save for the limited scenarios set out above, as opposed to a positive obligation whereby information relating to a customer's order must be disclosed. It is also noted that in contradistinction to the other examples raised in this article, the crossover between "personal data" as defined under the PDPA and information relating to a customer's order is minimal, and should not create significant practical difficulties in ensuring concurrent compliance with the regulatory regime under the Securities and Futures Act (and more specifically the Securities and Futures (Licensing and Conduct of Business) Regulations) as well as the PDPA.

## IV. Other practical considerations in handling customer personal data

16 With the growing prevalence of personal data in their role in helping to drive innovation in the FinTech industry, industry players must give heed to any concern, especially amongst the targeted consumer base, that organisations are not protecting their personal data and are instead using individuals' personal data in ways that do not correspond with the individuals' best interests.[19] These considerations should be in addition to obligations that are imposed on industry players via specific legislation. It is a delicate balancing act, and organisations should avoid viewing this as an arms race between advancements that exploit privacy in the name of

18 Cap 289, 2006 Rev Ed.

19 World Economic Forum, "Personal Data: The Emergence of a New Asset Class" (2011) at p 7.

innovation, and those that protect it at the risk of slowing advancements.[20] In fact, at any given point in time, new innovations from both camps are being created and introduced to the market, resulting in a constant fluidity in the balance of innovations in favour of and against privacy.[21]

17 In the light of this, there is certainly some benefit to the consideration that the merits or defects of particular technological advancements may not be rooted in the technology itself, but rather how the technology is being used and how its users are being held accountable.[22] Organisations should seek to ensure that a certain set of practical measures are in place and adhered to regardless of the individual product or technology in question. Some measures to consider include:

> (a) encrypting all communication channels, particularly where transmitting personal data, customer information or other sensitive or confidential information;
>
> (b) hashing sensitive information with a strong algorithm, to the extent possible;
>
> (c) avoiding retaining information for any longer than is absolutely necessary for the purposes for which it was collected; and
>
> (d) when sharing information with other entities (for example, service providers and related companies), seek to ensure that only information which is necessary is shared. For example, where an organisation looks to widen its social media reach through Facebook's look-alike audience functionality, the organisation will be required to share its existing customer base with Facebook. However, this information is hashed before being sent across to Facebook, where the hashed information is matched against the hashes of Facebook's existing user database to avoid any instance of "over sharing" as Facebook will only receive personal data which it already has (*ie*, collected from Facebook's existing users).

---

20 Amitai Etzioni, "Are New Technologies the Enemy of Privacy?" (2007) 20 *Knowledge, Technology & Policy* 115.

21 Amitai Etzioni, "Are New Technologies the Enemy of Privacy?" (2007) 20 *Knowledge, Technology & Policy* 115.

22 Amitai Etzioni, "Are New Technologies the Enemy of Privacy?" (2007) 20 *Knowledge, Technology & Policy* 115.

18 Organisations should also seek to implement clear and robust internal data management practices within the company. For example, certain personnel should be designated to be responsible for ensuring that the organisation collects, uses and discloses personal data and other information in a responsible manner that is compliant with all regulatory regimes. The roles and responsibilities of these individuals should be clearly and transparently defined, and they ought to familiarise themselves with the data collected and the data flows within the organisation. Organisations may also consider conducting regular training sessions to keep its employees abreast with developments in the various regulatory regimes, and ensuring that regular internal audits, assessments and reviews of the organisation's data management practices are undertaken in order to identify and rectify any gaps in compliance.

# DATA SHARING: WHEN CONSENT IS NOT ENOUGH*

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

**LEE Yue Lin**‡
*LLB (King's College London, University of London); Advocate and Solicitor (Singapore)*

## I. Introduction

1 In this technologically driven age, data is king.

2 Organisations have always shared data, even before the advent of data protection laws on our shores. Organisations may share personal data with each other for a multitude of reasons, from the desire to provide seamless healthcare services to the general population, to the need to carry out due diligence on individuals before processing financial transactions, or simply in order for organisations to provide individuals with more tailored and personalised services.

---

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

† Partner, WongPartnership LLP. Jeffrey's main areas of practice are in contentious and non-contentious intellectual property issues in the area of media, telecommunications, information technology, cybersecurity and data protection law. He is currently the Chairman of the Law Society's Project Law Help, the Vice Chair of the Law Society's Cybersecurity and Forensics Committee, as well as member of the Singapore Domain Name Dispute Resolution Policy (SDRP) Panel, the Singapore Academy of Law's Legal Technology Cluster Committee, the Law Society's Intellectual Property Committee and the Law Society's Information Technology Committee.

‡ Senior Associate, WongPartnership LLP. Yue Lin graduated from King's College London, the University of London, with an LLB (Hons) and was called to the Singapore Bar in 2013. Her main areas of practice are in intellectual property, media, telecommunications, information technology, cybersecurity and data protection law.

3 In the time before the passing of Singapore's Personal Data Protection Act 2012[1] ("PDPA"), organisations may (or may not) have sought consent from individuals before sharing their personal data with other organisations.

4 The PDPA has now established a consent-centric framework for the collection, use and/or disclosure of personal data by organisations.

5 In a nutshell, organisations which intend to collect, use and/or disclose the personal data of individuals must, *before* collecting, using and/or disclosing such personal data, ensure that they have (a) notified the individual of the purposes for which their personal data are being collected, used and/or disclosed, and (b) obtained their consent for such purposes[2] ("Consent Obligation").

6 Of course, there are exceptions to the Consent Obligation.

7 The PDPA also provides that if the collection, use or disclosure of personal data is required or authorised under the PDPA or any other written law, the consent of the individual is not required.[3] The Second, Third and Fourth Schedules to the PDPA set out the various situations under which an organisation may collect, use and/or disclose the personal data of an individual without the individual's consent.

8 However, as the situations listed under the Second, Third and Fourth Schedules to the PDPA are situation-specific (and sometimes subject to qualifiers),[4] organisations may be frustrated in their attempts to fit the purposes for which they wish to collect, use and/or disclose personal data within these exceptions.

---

1 Act 26 of 2012.

2 Personal Data Protection Act 2012 (Act 26 of 2012) ss 13(*a*), 14 and 20.

3 Personal Data Protection Act 2012 (Act 26 of 2012) s 13(*b*).

4 For example, para 1(*e*) of the Second Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012) provides that consent is not required from the individual where the "collection is necessary for any investigation or proceedings, if it is *reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data*" [emphasis added]. For an organisation to be able to rely on this exception, the organisation would need to first prove that (a) the collection of the personal data is in fact "necessary" for the investigation or proceedings, and (b) that it is "reasonable" to expect that seeking the consent of the individual would compromise the availability or accuracy of the personal data.

9 As the PDPA was enacted to govern the collection, use and disclosure of personal data by organisations, even where organisations seek to obtain the consent of individuals for the collection, use and/or disclosure of their personal data, organisations are required under the PDPA to ensure that the means by which consent is obtained meet certain requirements of reasonableness.[5]

10 This article will consider some of the objectives and limitations around the binary, consent-centric approach which Singapore's PDPA takes towards the collection, use and/or disclosure of personal data, as well as how other jurisdictions have approached this issue.

## II. Collection, use and disclosure of personal data under the Personal Data Protection Act

11 As discussed above, under the PDPA, organisations must, before collecting, using and/or disclosing personal data, first notify the individual of the purposes for which their personal data are being collected, used and/or disclosed, and obtain the individual's consent for such purposes while also bearing in mind the principle of reasonableness and other key requirements under the PDPA.[6]

---

5 Section 18(*a*) of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA") provides that an organisation may only collect, use or disclose personal data about an individual for purposes which "a reasonable person would consider appropriate in the circumstances". Section 11(1) further provides that in meeting its obligations under the PDPA, an organisation "shall consider what a reasonable person would consider appropriate in the circumstances". An example of the concept of reasonableness affecting the way in which consent must be obtained from individuals by organisations is captured in s 14(2), which provides 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*" [emphasis added].

6 For example, see the obligations regarding policies and practices which an organisation is required to develop and implement, set out in s 12 of the Personal Data Protection Act 2012 (Act 26 of 2012).

12 As such, an organisation wishing to collect, use and/or disclose the personal data of an individual must do the following:

> (a) notify the individual of the *reasonable* purposes for which the organisation will be collecting, using and/or disclosing their personal data;
>
> (b) obtain the individual's consent to such reasonable purposes; and
>
> (c) where the purposes would not necessarily be considered "reasonable to provide the product or service to that individual", notify the individual of these purposes and obtain consent for such purposes separately from the reasonable purposes.[7]

13 In addition, in order to adequately notify the individual of the purposes for which the organisation is collecting, using and/or disclosing their personal data, organisations would need to prepare a statement of these purposes. The PDPA does not specify the specific manner or form in which an organisation is to inform an individual of the purposes. However, the PDPC's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[8] ("Key Concepts Guidelines") advises that as good practice, organisations should state their purposes in a written form,[9] which in turn also facilitates the important practice of version control and tracking.[10]

14 Formulating such statements can, however, be a challenge, not only because of the great variety of purposes for which an organisation will today collect, use and/or disclose an individual's personal data, but also due to the fact that such purposes may evolve. As such, in a consent-centric regime, such statements have a tendency to become long and unwieldy as organisations attempt to meet the requirement to notify individuals (and thus comply with the Consent Obligation) while also enumerating as many purposes as reasonably possible to minimise the possibility that organisations will need to go back to the individuals at some later date for

---

7 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at paras 12.15–12.17.

8 Revised on 27 July 2017.

9 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at para 14.11.

10 The trend today seems to be for organisations to set out the purposes in written form through a data protection policy, which is incorporated by reference to/tied to a consent declaration/statement.

further consents where a new, reasonable purpose has arisen for which the organisation does not yet have the individual's consent.

15 Of course, there are limited situations in the PDPA pursuant to which an organisation can collect, use and/or disclose an individual's personal data without having to obtain further consent from the individual. These situations include, for example, where the organisation is disclosing the individual's personal data to its data intermediaries[11] to process the individual's personal data in accordance with the primary organisation's instructions,[12] or where the consent of the individual may be "deemed".[13]

16 Even here, the consent of the individual can only be deemed in very limited situations, *ie*, where:

> (a) the individual, without actually giving consent to the organisation in accordance with the PDPA, voluntarily provides the organisation with their personal data for that purpose, and "it is reasonable that the individual would voluntarily provide the data";[14] or
>
> (b) where an individual consents to the disclosure of their personal data by one organisation ("A") to another ("B")[15] – in other words, if an individual gives or is deemed to have given consent for disclosure of their personal data by A to B for a purpose, the individual is deemed to consent to the collection of their personal data by B for that purpose.

17 Indeed, the Key Concepts Guidelines emphasises that although organisations can choose to rely on deemed consent instead of obtaining actual consent from the individual, the preferred approach would still be for

---

11 Personal Data Protection Commission, *Guide to Data Sharing* (revised on 1 February 2018) at para 1.8.

12 However, the primary organisation should still enter into a written contract with the data intermediary (ss 4(2) and 4(3) of the Personal Data Protection Act 2012 (Act 26 of 2012)) to regulate the manner in which the data intermediary organisation processes the individual's personal data, and the data intermediary must not process the personal data for other purposes without the consent of the individual.

13 Personal Data Protection Act 2012 (Act 26 of 2012) s 15.

14 Personal Data Protection Act 2012 (Act 26 of 2012) s 15(1).

15 Personal Data Protection Act 2012 (Act 26 of 2012) s 15(2).

organisations to obtain actual consent instead of relying on deemed consent.[16]

18 Given the difficulties and limitations of applying deemed consent, organisations will be driven towards seeking actual consent from individuals for the collection, use and/or disclosure of their personal data, resulting in the long and unwieldy statements of purposes which may be counterproductive when the organisation is trying to notify individuals of the purposes for which their personal data are being collected, used and disclosed in a way that is easy to understand.

## III. Alternative ways of collecting, using and/or disclosing personal data under the Personal Data Protection Act

19 The PDPA provides alternatives for an organisation to collect, use and/or disclose the personal data of an individual without having to comply with the Consent Obligation.

20 Instead of obtaining consent, an organisation may:

(a) apply the statutory exceptions to the Consent Obligation available under the PDPA;
(b) anonymise the personal data which are collected, used and/or disclosed; or
(c) seek to be exempted from the Consent Obligation by the Personal Data Protection Commission ("PDPC").

We will consider each in turn.

### *A. Statutory exceptions to Consent Obligation*

21 The Second, Third and Fourth Schedules to the PDPA provide that in certain situations, organisations may collect, use and/or disclose the personal data of the individual without the individual's consent.

22 However, coming within these exceptions is easier said than done.

16 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at para 12.28.

23 The exceptions are largely qualified by the requirement of necessity. For example, an organisation can collect an individual's personal data without the consent of the individual for "any purpose that is clearly in the interest of the individual" provided that such collection is "necessary" for such purposes.[17] There has not been any case law in Singapore considering when something would be "necessary". "Necessity" is generally understood to refer to where an obligation cannot be performed in some other manner. In other words, to interpret the exception to the Consent Obligation in para 1(*a*) of the Second Schedule strictly, an organisation may only collect an individual's personal data for "any purpose that is clearly in the interest of the individual" where such collection is "*necessary*" for such purposes – and this term could cover a range of meanings including where there is no other way by which the personal data can be collected from the individual except without their consent, or where it is essential.

24 In addition, the exceptions to the Consent Obligation provided for in the Second, Third and Fourth Schedules to the PDPA are very situation-specific and may sometimes be further qualified by other requirements.

25 For example, an exception to the Consent Obligation relates to investigation or proceedings.[18] The exception provides that collection must be "necessary" for such investigations or proceedings, and "investigation" and "proceeding" have been specifically defined under the PDPA.[19]

---

17 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*a*).

18 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*e*).

19 "[I]nvestigation" is defined in s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) as follows:

> an investigation relating to —
>
> (*a*) a breach of an agreement;
>
> (*b*) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
>
> (*c*) a circumstance or conduct that may result in a remedy or relief being available under any law.

"[P]roceedings" is defined in s 2(1) as follows:

> any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of —

(*continued on next page*)

Organisations intending to collect an individual's personal data for the purpose of such investigations or proceedings must, before collecting the personal data, ensure that all of these requirements are met before they can collect an individual's personal data without the individual's consent.

26 Given the consent-centric framework of the PDPA, it is understandable that, in maintaining this approach, it should not be too easy for organisations to come within one of the available statutory exceptions. Conversely, it would also not be possible to exhaustively legislate exceptions to the Consent Obligation for all possible legitimate reasons through the existing statutory exceptions, even where it may not necessarily be desirable to obtain the notified consent of the individuals for such collection, use and/or disclosure.

27 Recently, the PDPC has proposed new approaches to consent in a consultation paper.[20] Briefly:

(a) **The "Deemed Consent by Notification Approach"**.[21] The PDPC has proposed that a notification-only approach can be taken by organisations collecting, using and disclosing personal data where the

---

(*a*) a breach of an agreement;

(*b*) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(*c*) a wrong or a breach of a duty for which a remedy is claimed under any law.

20 Personal Data Protection Commission, "Public Consultation for Approaches to Managing Personal Data in the Digital Economy" (27 July 2017) (hereinafter "Public Consultation on Digital Economy"); Personal Data Protection Commission, "Response to Feedback for Public Consultation on Approaches to Managing Personal Data in the Digital Economy" (1 February 2018) (hereinafter "PDPC Response on Digital Economy").

21 The "Deemed Consent by Notification Approach" was formerly referred to as the Notification of Purpose Approach in the Public Consultation on Digital Economy. See para 3.8 of the Public Consultation on Digital Economy for a description of the Notification of Purpose Approach and para 4.2(c) of the PDPC Response on Digital Economy for a description of the Deemed Consent by Notification Approach.

collection, use and disclosure of personal data is not expected to have any adverse impact on the individual.[22]

(b) **The "Legitimate Interests Basis"**. In addition to the Deemed Consent by Notification Approach, the PDPC has also proposed that organisations may, in addition to the existing exceptions to the Consent Obligation, collect, use or disclose personal data without the consent of the individual where there is a need to protect legitimate interests that will have economic, social, security or other benefits for the public (or a section thereof).[23]

In order to balance the protection of personal data with the needs of the businesses relying on either the Deemed Consent by Notification Approach or the Legitimate Interests Basis, the PDPC is proposing that organisations carry out a risk and impact analysis to assess the risks and impact of the intended collection, use and disclosure of personal data on the individual.

28 These proposed new approaches by the PDPC should go some way in easing the burden on organisations when they need to disclose an individual's personal data to other organisations for specific purposes. At the same time, it remains to be seen how organisations navigate, and whether they have the appetite to manage the requirements for constant and consistent risk and impact analyses, as well as the size of their appetites to rely on these new approaches to the collection, use and disclosure of personal data.

### *B. Anonymising personal data*

29 If the organisation is unable or unwilling to comply with the Consent Obligation but is also unable to fit the purposes for which they intend to collect, use and/or disclose the personal data within a statutory exception to consent, another alternative is for the organisation to anonymise the personal data so that the data collected fall outside the framework of the PDPA.

---

22 Public Consultation on Digital Economy at para 3.8(b); PDPC Response on Digital Economy at paras 4.2(c) and 6.4.

23 PDPC Response to Digital Economy at para 5.7.

30 Given the broad and inclusive definition of "personal data" under the PDPA[24] and the volume of personal data which an organisation tends to collect from individuals today, it may not necessarily be enough for an organisation to merely anonymise only the specific set of data which it is collecting from the individual in that instance, particularly if the anonymised set can still be converted back to personal data based on "other information to which the organisation *has or is likely to have access*" [emphasis added]. As such, any anonymisation of personal data by an organisation will likely require, among other things, the establishment of "robust organisational, legal and non-technical measures to manage the risks of re-identification".[25]

31 In addition, given that many of the goods and services provided by organisations today are personalised to the individual, the value of processing only anonymised data may be questionable. Indeed, as "big data" applications proliferate, the commercial use cases and economic value of customised consumer experiences are both realities and propositions which drive the pressure to develop new alternatives to the consent-centric regime.

### *C. The Personal Data Protection Commission's exemption from Consent Obligation*

32 Section 62 of the PDPA empowers the PDPC to exempt "any person or organisation … from all or any of the provisions of [the PDPA]".

33 The PDPC has, in its recent *Guide to Data Sharing*,[26] provided for the considerations and criteria pursuant to which an organisation may apply to the PDPC for their data sharing arrangements to be exempted from the provisions of the PDPA "on a case-by-case basis".[27]

---

24 "Personal data" is defined in s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) as "data, whether true or not, about an individual who can be identified (*a*) from that data; or (*b*) from that data and other information to which the organisation has or is likely to have access".

25 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised on 28 March 2017) at para 3.25.

26 Revised on 1 February 2018.

27 Personal Data Protection Commission, *Guide to Data Sharing* (revised on 1 February 2018) at para 3.14.

34 Pursuant to the *Guide to Data Sharing*, a data-sharing arrangement between organisations may be exempt from, for example, the Consent Obligation where the following criteria are met:[28]

> (a) The personal data shared under the data-sharing arrangement must be with a specified group of organisations for a specified period of time, and this must be stated in the application. After an exemption is granted, if additional organisations need to be added to the data-sharing arrangement, approval must be sought from the PDPC.
>
> (b) The purposes of the data-sharing arrangement must be defined and specific.
>
> (c) The sharing must not be likely to have any adverse impact on the individuals, or there are legitimate purposes for the sharing and the benefits to the public (or a section thereof) which outweigh any foreseeable adverse impact on the individuals.

35 Organisations which obtain an exemption from complying with the Consent Obligation from the PDPC pursuant to s 62 of the PDPA will be able to share individuals' personal data with other organisations without having regard to the Consent Obligation.

36 However, organisations are still required to submit an application to the PDPC, and the exemption, once granted, would only apply for a "specified period of time".

37 While these administrative steps may act as safeguards and ensure that organisations do not abuse the exemptions granted to them, the burden of complying with these steps and, in particular, limiting the data-sharing arrangement to a specified time period, may stifle organisations' ability to take full advantage of any exemption which may be granted by the PDPC.

## IV. What other jurisdictions are doing

38 We have seen that it is difficult, in a consent-centric regime, to balance the needs of organisations with the protection of an individual's personal data.

---

28 Personal Data Protection Commission, *Guide to Data Sharing* (revised on 1 February 2018) at paras 3.15–3.17.

39 How do other jurisdictions ensure that businesses continue to be able to collect, use and/or disclose the personal data of individuals while ensuring that organisations provide adequate protection to such personal data?

40 A number of other jurisdictions do encourage organisations to process personal data on grounds *other than* consent. These will be briefly discussed here, highlighting a few examples.

41 In some jurisdictions, an emphasis is placed on notifying the individual of the purposes for which their personal data are being processed by organisations, and the onus is placed more firmly on organisations to determine for themselves whether the purposes for which they are processing personal data come within the statutory framework provided by the relevant data protection legislation. In the European Union, for example, the General Data Protection Regulation ("GDPR")[29] provides for organisations to process the personal data of individuals on a number of grounds, consent being only *one* of the possible grounds. Some examples of the grounds upon which organisations may process the personal data of individuals include the following:[30]

> (a) the individual has given consent[31] to the processing of one or more specific purposes;
>
> (b) the processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;
>
> (c) the processing is necessary for compliance with a legal obligation to which the controller is subject;

29 Personal data protection has, for many years, been regulated by the EC Directive 95/46/EC ("Data Protection Directive"). The core rules relating to the grounds upon which an individual's personal data may be processed under the General Data Protection Regulation (EU) 2016/679 and the Data Protection Directive remain broadly the same.

30 General Data Protection Regulation (EU) 2016/679 Art 6(1).

31 Perhaps owing to the fact that organisations subject to the General Data Protection Regulation (EU) 2016/679 ("GDPR") are able to process personal data on various grounds including consent, valid consent is also much harder to obtain under the GDPR – see Recitals 32, 42 and 43.

(d) the processing is necessary for the purposes of the legitimate interests[32] pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal data, in particular where the data subject is a child.

42 Similarly under Australia's Federal Privacy Act 1988 (Cth) ("FPA"), the consent of the individual is required only in certain limited situations,[33] and the onus seems to be placed on each organisation to regulate its own collection, use and disclosure of personal data in accordance with the Australian Privacy Principles ("APPs") enshrined in the FPA.[34]

---

32 Organisations are left to determine whether a particular purpose would constitute a "legitimate interest" of the organisation.

Interestingly for organisations seeking to process the personal data of individuals on grounds other than consent under the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the GDPR has also provided some useful examples of what would constitute the "legitimate interest" of an organisation. Recitals 47 to 49 provide that the legitimate interests of organisations may include, among others, the processing of personal data strictly necessary for the purposes of preventing fraud, for direct marketing purposes, the transmission of personal data between organisations that are part of the same group of companies or which are affiliated to a central body, for internal administrative purposes, or the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security.

33 Australian Privacy Principles 3, 5 and 6.

34 Personal data must be collected by organisations only in so far as such collection is reasonably necessary for one or more of the organisation's functions or activities, and the organisation collecting the personal data, must, at the time before the personal data are collected, or as soon as practicable afterwards, notify the individual of, among other things:

(a) the organisation's identity and how to contact it;
(b) why the organisation is collecting (or how it will use the) information about the individual;
(c) to whom the organisation might give the personal data;
(d) any law requiring the collection of personal data;
(e) the main consequences (if any) for the individual if all or part of the information is not provided; and
(f) the fact that the organisation's data protection policy contains information about how the individual may access and seek correction

(*continued on next page*)

43 Notwithstanding the more permissive processing regimes under the GDPR and the FPA, individuals' rights are still safeguarded.

44 Balance is provided under the GDPR in the following ways:

(a) organisations regulated by the GDPR are required to consider the question of whether the processing is "necessary" for the stated purposes, in addition to the requirement that organisations seeking to process personal data on grounds of "legitimate interest" are required to consider whether these interests are overridden by the interests or fundamental rights and freedoms of the individual which would require the protection of that personal data;

(b) individuals are given the right to object to the processing, subject to certain requirements being met;[35] and

(c) heavy fines are imposed on organisations in breach of their obligations under the GDPR.[36]

45 In Australia, the federal Privacy Commissioner is granted a range of powers under the FPA, including the power to make a determination after an investigation, including a determination as to the range of remedies that should apply, the power to seek civil penalties, the power to seek an injunction to prevent privacy breaches and the power to seek an enforceable undertaking as to an organisation's compliance with the FPA.[37]

46 Having regard to the above, the path to a non-consent-centric regime is paved by a balancing of interests – fortifying other data protection obligations, strengthening the enforcement regime, importing concepts such as "necessity", *etc*.

47 In this light, one point to consider therefore is whether the removal of the need to procure consent means that the data subject's right to object to or require the cessation of the collection, use or disclosure of personal data

---

of their personal data, how they may make a complaint about a breach of the Australian Privacy Principles and how the organisation will deal with such complaint.

35 General Data Protection Regulation (EU) 2016/679 Art 21.

36 As an example, fines of up to 4% of annual worldwide turnover or €20m, whichever is greater, may be imposed on an organisation. See Art 83(5) of the General Data Protection Regulation (EU) 2016/679.

37 Federal Privacy Act 1988 (Cth) (Australia) ss 40, 52 and 98.

has been curtailed. After all, in a consent-centric regime, the data subject's rights would have been protected by granting them the right to withdraw consent. That option does not exist if the legal framework were not consent-based in the first place.

48 Would the balancing step in a non-consent-centric approach be to provide for a right for the data subject to subsequently require that collection, use or disclosure for unconsented purposes cease? How would such a right be structured so as to be feasible and minimise hurdles for organisations or individuals?

## V. Conclusion

49 For the time being, Singapore's PDPA remains a largely consent-centric regime. Perhaps with advancements in technology and the introduction of dynamic consents through which individuals can be given greater control over the types of consent they wish to give to organisations processing their personal data, the burden of compliance will be eased.

50 However, as we have seen from other jurisdictions, there are many ways to protect an individual's personal data and still facilitate the conduct of business.

51 As Singapore's data protection landscape matures, there is now perhaps room to implement a more permissive data protection framework under which organisations will be freer to collect, use, disclose and process personal data on grounds beyond consent, and yet where the protection of the individual's personal data is still guaranteed. Diversifying the means to secure the rights to collect, use or disclose data whilst striking a balance of interests between organisations and individuals would certainly be a progressive step in this regard.

# PROTECTING CONSUMERS' PERSONAL DATA IN THE DIGITAL WORLD – CHALLENGES AND CHANGES*

**YIP Man**†
*LLB (Hons) (National University of Singapore), BCL (Oxford); Advocate and Solicitor (Singapore)*

## I. Introduction

1 At the Personal Data Protection Seminar 2017, Dr Yaacob Ibrahim, Minister for Communications and Information, said that Singapore must "aspire towards a high standard of data protection that strengthens trust with the public, gives confidence to customers whose data is collected and used, while providing an environment for companies to thrive in the digital economy".[1] In his speech, he acknowledged that the Personal Data Protection Act 2012[2] ("PDPA") was crafted in an era where the majority of the data were derived from physical or online form filling exercises. The age we are in, however, is where data are being constantly generated and mined through transactions and activities on the Internet and other forms of technology.[3] The digital economy is built on the model of *efficient data sharing*. Dr Yaacob Ibrahim thus calls for a change in data protection mindset and culture: to move from compliance to accountability.

---

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

† Associate Professor of Law, School of Law, Singapore Management University. Yip Man is the Deputy Director of the Centre for Cross-Border Commercial Law in Asia, the Asia Pacific Digest Editor for the *Restitution Law Review* and a co-Administrator of the Singapore Law Blog. She previously served as a member of the Singapore Academy of Law Law Reform Committee.

1 Dr Yaacob Ibrahim, Minister for Communications and Information, "From Compliance to Accountability: A Robust and Progressive Data Protection Framework" Personal Data Protection Seminar 2017 (27 July 2017) <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2017/7/personal-data-protection-seminar-2017> (accessed on 11 January 2018).

2 Act 26 of 2012.

3 For example, the facial recognition technology.

Businesses are to play an active role, in partnership with the Personal Data Protection Commission ("PDPC"), in protecting their customers' data. The focus shifts from regulator to data controller.

2 Thus far, the PDPC is taking swift action to help build and strengthen industry accountability in respect of the harvest, use and transfer of consumer data.[4] The emphasis of the proposed approach[5] is in part targeted at businesses' obligations (data breach mandatory notification) and business accountability under an enhanced framework for the collection, use and disclosure of personal data[6] (for example, conducting a risk and impact assessment). Indeed, the mandatory obligation to notify of data breach is part of enforcing greater business accountability. Elsewhere, in Europe and the US, legislative proposals have adopted a different strategy by placing control in data subjects (*ie*, consumers). These are crucial, though initial, steps to kickstarting the change in the mindset and culture of data protection.

4 "Data Privacy Laws Changing in Tune with Digital Economy" *The Straits Times* (28 July 2017).

5 See Personal Data Protection Commission, "Public Consultation for Approaches to Managing Personal Data in the Digital Economy" (27 July 2017) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthedigitaleconomy270717f95e65c8844062038829ff000.pdf> (accessed 17 March 2018); Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in Digital Economy" (1 February 2018) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf> (accessed 17 March 2018).

6 The enhanced framework allows for the collection, use and disclosure of personal data (a) through deemed consent by notification of purpose or (b) without consent on the basis of "legitimate interests".

3 This article discusses challenges that require us to rethink the present regulatory approach and explores what more can be done in the future. The starting point is a clear acknowledgment of two facts:[7] data are the bloodline of the digital economy; and data processing by businesses or data sharing between businesses may be beneficial to consumers. An unduly restrictive approach would stifle innovation and undermine the value which the appropriate and legitimate use of data could bring to society. This article argues that we should adopt a multi-pronged, balanced approach of placing responsibility on the regulator, businesses as well as the consumers themselves for consumer data protection.

## II. Challenges

4 To skillfully navigate the challenges posed by the digital world, we must first understand what these challenges are.[8] As a starting point, there are four obvious challenges in respect of regulating the protection of consumers' data in the digital marketplace. The first challenge is the difficulty of using consent as an effective means of authorising the collection and use of data in the digital world. One constraint is the inefficiency from having to obtain consent constantly. It has been pointed out that "an overemphasis of autonomous authorisation" will lead to an overload of consent transactions[9] with the consequence that consumers suffer from "consent fatigue" and "consent desensitisation", rendering consent an ineffective authorisation mechanism.[10] Indeed, the PDPA does not overemphasise the role of consent in data protection.[11] The PDPC's proposed reform of introducing "Notification of Purpose", in the absence

7 The UK government has acknowledged these two facts in mapping out its strategy for "unlocking the power of data in the UK economy and improving public confidence in its use". See *UK Digital Strategy 2017* (1 March 2017) section 7 <https://www.gov.uk/government/publications/uk-digital-strategy> (accessed 17 March 2018).

8 Undoubtedly, new challenges will continue to arise.

9 This problem is particularly acute in the context of Internet activities.

10 B W Shermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171 at 176–179.

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

of obtaining consent, as an appropriate basis for data collection, use or disclosure acknowledges that in some circumstances it may be impractical to obtain consent.[12] The other problem with over-reliance on consent is related to technological advancement. As Hermstrüwer explains, the individualistic conception of privacy "misses a crucial feature of modern data analytics (Big Data) and the behavioral forces underlying the diffusion of personal information in networked environments". That is, in a networked environment, it is possible to predict, on the basis of probabilities, the traits of users, who did not disclose their personal information, based on the personal information disclosed by these individuals' friends in the same environment by running a simple logistic regression based on certain parameters.[13] A further technological challenge to obtaining consent is the design of the technological device itself: people frequently conduct transactions over their mobile phones and the size of the screen poses a significant challenge for obtaining meaningful consent. Moreover, it is well established that the readership of terms and conditions for online consumer contracting is very low.[14] The consumer may thus

12 See Personal Data Protection Commission, "Public Consultation for Approaches to Managing Personal Data in the Digital Economy" (27 July 2017) at para 3.8.

13 Yoan Hermstrüwer, "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data" (2017) 8 *Journal of Intellectual Property, Information Technology and Electric Commerce Law* 9 at 12–13. The more information disclosed by the friends, the higher the probability of determining the personal information relating to the users who did not consent to the disclosure. See also, UK Government Office for Science, "Artificial Intelligence: Opportunities and Implications for the Future of Decision Making" (9 November 2016) at p 14 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf> (accessed 17 March 2018).

14 European Commission, "Study on Consumers' Attitude Towards Terms and Conditions (T&Cs): Final Report" (Brussels 2016) at p 9 <http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/terms_and_conditions_final_report_en.pdf> (accessed 17 March 2018); Yannis Bakos, Florencia Marotta-Wurgler & David R Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts" (2014) 43 *Journal of Legal Studies* 1.

blindly or without consideration accept unfair or onerous terms on the processing and use of their data.[15]

5 Second, online business strategies, prompted by technological developments, may make it harder for consumers to realise that their personal data are being harvested, stored and/or used. In particular, many online "free" services are not provided by businesses free of charge but are in exchange for the consumer's disclosure of personal data. These businesses' main source of revenue is advertising; and consumers' data could help them improve and enhance their advertising strategies (for example, customer churn prediction, targeted advertising or interest-based advertising) for companies who sought the advertising service. Facebook, Google and Instagram are notable examples of businesses that operate on such a model. Yet, there is real concern that consumers are unaware of how their data will be used by the businesses.

6 Thirdly, business models are also evolving rapidly. Buzz terms like "sharing" economy,[16] collaborative economy, collaborative consumption and on-demand services[17] are emblematic of the change that is swiftly taking place. Singapore's attitude is to embrace such innovations and the associated technologies. Liu Feng-Yuan, Director of the Government Technology Agency of Singapore's Data Science Division, said: "From a public good point of view, we're really keen on encouraging these technologies. The sharing economy is about better utilisation, better sharing

15 Stephanie Law, "At the Cross-roads of Consumer Protection, Data Protection and Private International Law: Some Remarks on *Verein fur Konsumenteninformation v Amazon EU*" (2017) 45 *European Law Review* 751 at 765.

16 See generally Lisa Gansky, "How the Sharing Economy Can Create Value from Waste" *Huffington Post* (11 October 2015) <https://www.huffingtonpost.com/lisa-gansky/sharing-economy-value-waste_b_8522490.html> (accessed 17 March 2018).

17 For definitions, see Rachel Botsman, "Defining the Sharing Economy: What is Collaborative Consumpion – And What Isn't?" (27 May 2015) <https://www.fastcompany.com/3046119/defining-the-sharing-economy-what-is-collaborative-consumption-and-what-isnt> (accessed 17 March 2018).

and better services for the people."[18] However, such business models raise data protection concerns as the companies which own these platforms are in possession of large volumes of personal data of the users.

7 Finally, there is an acceleration of concentration of power over data in the hands of corporate giants,[19] such as Amazon, Apple, Facebook and Google. Facebook has been embroiled in online privacy controversies since its takeover of WhatsApp in 2014. It has been fined €110m by the European Commission for providing incorrect or misleading information[20] on the possibility of data sharing between Facebook and WhatsApp.[21] It has also come under investigations and scrutiny by several national data protection and/or competition authorities in the European Union ("EU").[22] Further, it has been observed that five companies – Alphabet, Amazon, Apple, Facebook and Microsoft – have dominant control, through acquisitions of startups, over the talent and intellectual property behind the emerging field of artificial intelligence ("AI") and machine learning.[23] One concern is that these companies "sit on vast stores of user data that are

18 "The Sharing Economy of Data" (30 June 2017) <https://www.tech.gov.sg/TechNews/Innovation/2017/06/The-sharing-economy-of-Data> (accessed 17 March 2018).

19 See generally Giovanni Buttarelli, "Strange Bedfellows: Data Protection, Privacy and Competition" (2017) 13 *Competition Law International* 21 at 22–23.

20 See European Commission Press Release, "Mergers: Commission Alleges Facebook Provided Misleading Information about WhatsApp Takeover" (Brussels, 20 December 2016) <http://europa.eu/rapid/press-release_IP-16-4473_en.htm> (accessed 17 March 2018).

21 See news report by CNBC: <https://www.cnbc.com/2017/05/18/facebook-fine-eu-whatsapp-takeover.html> (accessed 17 March 2018).

22 See, for example: <https://www.theguardian.com/technology/2017/dec/19/facebook-use-of-third-party-apps-violates-data-protection-principles> (Germany); <https://www.theguardian.com/technology/2017/dec/19/france-orders-whatsapp-stop-sharing-user-data-facebook-without-consent> (France); and <https://www.bloomberg.com/news/articles/2017-10-12/facebook-is-watching-you-belgian-privacy-agency-warns-in-court> (Belgium) (accessed 17 March 2018).

23 Vinod Iyengar, "Why AI Consolidation Will Create the Worst Monopoly in US History" (24 August 2016) <https://techcrunch.com/2016/08/24/why-ai-consolidation-will-create-the-worst-monopoly-in-us-history/> (accessed 17 March 2018).

rivaled only by governments".[24] The trend of such power concentration in large private companies sets off alarm bells on the transparency of these companies' activities, in particular, how regulators could effectively monitor their collection, use and transfer of personal data. Transformative technological advancements such as AI and machine learning – which enable automated decision-making – could easily outstrip the pace of regulatory reform, thereby exacerbating the problem. Regulatory response is reactionary. As Commissioner Pamela Jones Harbour put it in her dissenting statement in respect of Google's acquisition of DoubleClick:[25]

> The truth is, we really do not know what Google/DoubleClick can or will do with its trove of information about consumers' Internet habits. The merger creates a firm with vast knowledge of consumer preferences, subject to very little accountability. [reference omitted]

8 The market monopoly trend also signals the need for competition regulators to assess economic activities with consumer protection and data protection angles in mind. As such, collaboration amongst these three authorities would be sensible.

## III. New regulatory philosophy: Enabling individual control, shared responsibility and enhancing trust

### *A. EU General Data Protection Regulation*

9 Against these challenges highlighted above and other challenges that are associated with the digital environment, a new regulatory philosophy begins to emerge. This is evident in the new regime set out in the EU's General Data Protection Regulation ("GDPR"). The GDPR, which will replace 28 local laws in the EU Member States, will take effect in May

---

24 Vinod Iyengar, "Why AI Consolidation Will Create the Worst Monopoly in US History" (24 August 2016) <https://techcrunch.com/2016/08/24/why-ai-consolidation-will-create-the-worst-monopoly-in-us-history/> (accessed 17 March 2018).

25 Dissenting judgment of Commissioner Pamela Jones Harbour in *In the matter of Google/DoubleClick* (FTC File No 071-0170) at p 10 <https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf> (accessed 17 March 2018).

2018. The GDPR is marked by a number of key changes.[26] Five changes – relevant to the present discussion – will be highlighted. First, it increases the territorial scope of application, covering all businesses (whether situated within or outside of the EU)[27] which process the personal data of data subjects residing in the EU. Second, higher penalties are imposed on breaches of the rules, with the maximum fine being 4% of a company's total global turnover. Third, the new regime enhances the role of consent by strengthening the conditions for obtaining consent from data subjects.[28] Article 12 of the GDPR obliges the companies to provide information to users "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". Fourth, the GDPR prescribes a broad range of rights for data subjects,[29] including the right to rectification and erasure, right to restrict processing, right to data access and right to data portability. Fifth, the GDPR shifts the responsibility of personal data protection on data controllers and processors[30] by prescribing a number of obligations, including mandatory data breach notification, the requirement to design systems with data protection from the outset and the obligation to put in place data protection officers.

10 The GDPR has received mixed reviews, with some considering it to be overly heavy-handed, thereby increasing the costs of compliance for businesses[31] – a consequence that would be most severely felt by smaller

26 For a summary, see <https://www.eugdpr.org/key-changes.html> (accessed 17 March 2018).

27 For a summary of key aspects of the legislation, see <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/eu-gdpr-factsheet--041017.pdf> (accessed 17 March 2018).

28 *Cf* Yoan Hermstrüwer, "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data" (2017) 8 *Journal of Intellectual Property, Information Technology and Electric Commerce Law* 9 at 17. Hermstrüwer argues that the transparency obligation does not sufficiently address the information asymmetries between companies and customers and it is inconsistent with the requirement regarding the kind and quantity of information that must be made available to customers under Art 14 of the European Union General Data Protection Regulation.

29 European Union General Data Protection Regulation Ch 3.

30 European Union General Data Protection Regulation Ch 4.

31 "Data Protection: Brussels' Heavy Hand on Europe's Digital Economy" *Financial Times* (22 November 2017).

businesses. The discussion here is not focused on the shortcomings of the new regime. Rather, what is not to be missed is the regulatory shift towards enabling the data subjects to control the use of their data through the provision of a range of rights and putting heavier responsibility on data controllers/processors through the provision of a range of obligations. Importantly, these obligations on controllers/processors systematically require these actors to integrate data protection into their business models. As such, the emerging regulatory picture is one of shared responsibility between the regulator, the controller/processor and the data subject (*ie*, the consumers).

### *B. US Consumer Privacy Bill of Rights*

11 The Obama administration put forward the Consumer Privacy Bill of Rights in 2012 to improve privacy protection for consumers; the same was reintroduced again in 2015.[32] The Consumer Privacy Bill of Rights 2012 provides blueprint guidance on enhancing online privacy protection, setting out seven basic "rights": "(1) individual control; (2) transparency; (3) respect for context; (4) security; (5) access and accuracy; (6) focused collection; and (7) accountability".[33]

12 The intentional paradigm shift that was made in the Consumer Privacy Bill of Rights was the emphasis on the consumers' rights.[34] In particular, the right to individual control has two core aspects: "'providing customers with easily used and accessible mechanisms' with which to exercise control and two, 'consumer responsibility', which recognises that the use of personal data turn upon the individual's decision to share data with others".[35] Commentators have thus said that this amounts to enabling

32 See <https://www.whitecase.com/publications/article/white-house-re-introduces-consumer-privacy-bill-rights-act> (accessed 17 March 2018).

33 Hakeem Rizk, "Fundamental Right or Liberty: Online Privacy's Theory for Co-Existence with Social Media" (2013) 56 *Howard Law Journal* 951.

34 "Why a Push for Online Privacy is Bogged Down in Washington" *New York Times* (28 February 2016). See also George Jepsen, "Big Data and Insurance Symposium" (2014) 21 *Connecticut Insurance Law Journal* 255 at 258–259.

35 Andy Crabtree *et al*, "Enabling the New Economic Actor: Data Protection, the Digital Economy and the Databox" (2016) 20 *Pers Ubiquit Comput* 947 at 950.

a new economic actor, the data subject, in the data protection process, an aspect that is also evident in the EU approach discussed above.[36]

13 The Consumer Privacy Bill of Rights further proposed a more vigorous participation scheme in the form of a "parallel self-regulatory process".[37] This self-regulatory process, operating under the Commerce Department, was to involve both businesses and consumer groups working together to "devise voluntary privacy practices for mobile apps, drones and other technologies".[38] This proposal clearly recognised the need for shared responsibility in data protection and to better facilitate the consumers' voice to be heard in the process.

### C. *Building trust*

14 Societal attitudes towards data sharing are also changing. People are becoming more accepting towards the practice of disclosing personal information in exchange for services or before making purchases online.[39] The most important factor for consumers' willingness to share personal data is their trust in the business. As such, a regulatory approach that focuses on business accountability and requiring businesses to build data protection into their business design is a step in the right direction. Beyond legal requirements, in the light of survey findings, businesses should be incentivised to take further action to build the customers' trust in their data protection practices. As such, self-regulation by businesses may be the most timeous and effective solution to some of the challenges arising in the age of big data and the digital economy.

---

36 Andy Crabtree *et al*, "Enabling the New Economic Actor: Data Protection, the Digital Economy and the Databox" (2016) 20 *Pers Ubiquit Comput* 947 at 950.

37 "Why a Push for Online Privacy is Bogged Down in Washington" *New York Times* (28 February 2016).

38 "Why a Push for Online Privacy is Bogged Down in Washington" *New York Times* (28 February 2016).

39 "What Marketers Need to Know About Consumers' Attitudes to Sharing Data" *The Guardian* (9 July 2015). See also <https://www8.gsb.columbia.edu/newsroom/newsn/3850/study-shows-that-consumers-are-willing-to-share-personal-data-if-the-benefits-and-brand-are-right> (accessed 17 March 2018).

## VI. Going forward: Other concerns

15 The discussion above has highlighted the main challenges to data protection brought about by the digital world and technological advancements. It has also analysed the rise of a new regulatory philosophy that is built upon the core concepts of consumer control, shared responsibility and trust. Of course, these core concepts could be implemented in practice in various ways, and not necessarily all efforts are to be undertaken by the PDPC alone. For example, industry can play a more active role in the development of sector-specific data protection requirements or coming together to formulate core responsible corporate practices. Indeed, many businesses have overseas operations and are thus confronted with the issue of having to meet the privacy regulatory requirements of different jurisdictions. Whether companies should adopt a fragmented corporate response for each jurisdiction or a uniform, multi-jurisdictional corporate response is a matter that is best left to businesses to decide. In this regard, major industry players can take on a thought leadership role.[40] It may also be that parallel/facilitative processes could be set up by related agencies, for example, establishing an awards scheme to recognise businesses that innovate data protection practices.[41] This scheme would not only reward businesses and help them in building greater public confidence, it would also foster a local culture of self-regulation and industry-driven code of good practices.

16 Further, going forward, there are other concerns to address. First, attention must be paid to the international dimension of data protection. The Internet and other technologies have made it easy to carry out cross-border transfers or processing of personal data. National legislation alone would not be sufficient to combat abusive use or processing of data. Regional co-operation and consensus would be necessary.[42] In this regard,

40 See Advertorial: "Personal Data Protection: An Intrinsic Priority of Singapore's Largest Bank" *Business Tmes* (9 January 2017).

41 The Personal Data Protection Commission has announced plans to introduce the Data Protection Trustmark Certification Scheme by end 2018. See <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Press-Room/2017/pdps2017-media-release---(260717).pdf> (accessed 17 March 2018).

42 See "Consumer Protection in E-commerce: OECD Recommendation" (2016) at para 54 <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf> (accessed 17 March 2018).

Singapore has recently become[43] a member of both the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules System[44] and the APEC Privacy Recognition for Processors System.[45] Other steps could include building a collaboration network amongst the national data protection agencies in the region to share, within legal limits, information and experiences.

17 Second, greater co-operation and communication between competition, data protection and consumer protection agencies can be fostered. This ensures that policies would be devised with a more holistic perspective on the impact and implication of certain economic activities.

18 Third, there is a need to focus on developing effective dispute resolution rules and mechanisms for e-commerce consumers in domestic and international disputes. Special attention should be paid to rules on jurisdiction, choice of law and rules to determine if jurisdiction clauses and choice of law clauses are unfair to the consumer who has no opportunity or ability to negotiate these terms. These rules have an impact on the level of data protection for the consumers. Further, dispute resolution mechanisms for e-commerce consumers should be effective, efficient, user-friendly, transparent and cost-friendly.[46] Singapore, as the incumbent Chair of the Association of Southeast Asian Nations ("ASEAN") for 2018, could leverage on the ASEAN infrastructure to push forward the agenda as well as enhance regional co-operation. In this connection, it is noteworthy that the ASEAN Economic Community Blueprint 2025 considers the need to devise correlated strategic measures relating to the rise of e-commerce, in particular, measures targeted at consumer protection, online dispute

43 See the Personal Data Protection Commission's announcement on 6 March 2018 <https://www.pdpc.gov.sg/pdpc/news/press-room/2018/03/singapore-joins-apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems> (accessed 17 March 2018).

44 Singapore is the sixth member. Other members are Canada, Japan, Korea, Mexico and the US.

45 Singapore is the second member, after the US.

46 See "Consumer Protection in E-commerce: OECD Recommendation" (2016) at paras 43–45 <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf> (accessed 17 March 2018).

resolution for e-commerce and personal data protection.[47] Moreover, Singapore's priority focus for 2018 as ASEAN chair is improving ASEAN economic connectivity through the digital economy.[48]

19 Finally, Singapore should promote more focused research on data science, behavioural science on decision-making of consumers as well as sociological empirical research on consumer attitudes. These research studies would greatly aid regulators in deciding the best regulatory and non-regulatory responses to new challenges in the digital world.

## VII. Conclusion

20 The rapid rise of digital economy has brought both benefits and challenges. It is important to recognise what these challenges are. It is equally important to embrace necessary changes to respond to the challenges. Whilst the PDPA has laid down the baseline framework for personal data protection, we are clearly in the next phase of regulatory challenge and innovation.

21 In *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*, the authors said:[49]

> Data was no longer regarded as static or stale, whose usefulness was finished once the purpose for which it was collected was achieved … Rather, data became a raw material of business, a vital economic input, used to create a new form of economic value. In fact, with the right mindset, data can be cleverly reused to become a fountain of innovation and new services. The data can reveal secrets to those with the humility, the willingness, and the tools to listen.

22 This article points out that we need to embrace a new mindset in effectively handling the challenges generated by the age of big data and the digital economy. The responsibility of enabling data to become "a fountain

---

47 ASEAN Economic Community Blueprint 2025 at para 53 <http://www.asean.org/storage/images/2015/November/aec-page/AEC-Blueprint-2025-FINAL.pdf> (accessed 17 March 2018).

48 "Singapore to Focus on Digital Economy, Trade Facilitation as ASEAN Chair in 2018" *Business Times* (12 September 2017).

49 Victor Mayer-Schonberger & Kenneth Cukier, *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight* (John Murray, 2017) at p 5.

of innovation and new services" is to be shared between the regulator, the businesses and the consumers. Everyone must participate to derive the maximum benefits promised by the new economy.

# CLOUD COMPUTING AND INTERNATIONAL DATA TRANSFERS UNDER THE PERSONAL DATA PROTECTION ACT*

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

**SZE TOH Kai Siang**
*Bachelor of Applied Science (Computer Engineering); CIPT*

## I. Introduction

1 With the proliferation of the use of cloud computing in the latest technology and gadgetry – from mobile cloud applications to cloud-based healthcare monitoring systems – data protection rules governing international data transfers have grown of immense importance. As one author has observed, cloud computing is one of the factors leading to the increase in volume of personal data transfers internationally.[1]

2 When it comes to complying with the transfer limitation obligation[2] ("Transfer Limitation Obligation") under the Personal Data Protection Act 2012[3] ("PDPA") for cloud computing, there are a number of approaches available to organisations. This article explores the considerations behind these approaches. Finally, the article will offer views on how this area of law may be improved to be more conducive to cloud computing.

---

* 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.

† Senior Associate, LVM Law Chambers LLC.

1 Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013) at p 3.

2 As defined at para 10.2(h) of the Personal Data Protection Commission, *Advisory Guidelines on the Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017).

3 Act 26 of 2012.

3 As the area on international data transfers in the cloud encompasses a wide range of data protection issues, this article does not seek to cover all these issues, and will focus mainly on the issues relating to compliance with the Transfer Limitation Obligation for cloud computing.

## II. What is cloud computing?

4 Cloud computing is a model for enabling access to a shared pool of computing resources that can be rapidly provisioned and released.[4]

5 There are three main service models of cloud computing: Infrastructure-as-a-Service ("IaaS"), Platform-as-a-Service ("PaaS") and Software-as-a-Service ("SaaS"). IaaS offers computing infrastructure such as processing power and/or storage to customers and consumers who are responsible for installing their own operating systems and applications. PaaS offers a platform and tools to customers so that they can construct, install and develop their own applications. SaaS provides end-users with "ready to use" software applications.[5]

6 There are four major cloud deployment models – public, private, community and hybrid. This refers to the scheme of resource sharing, for example, private cloud is meant for use within the organisation, while community cloud would refer to organisations within a specific community that can be managed by either a third party or the community itself, and can be hosted off-site or within the community's premises.[6]

7 The main characteristic of cloud computing is that it allows an organisation to tap into a shared pool of computing resources that may span multiple geographical locations depending on factors like cost effectiveness, *ie*, hosting the server in another country, or geographical resiliency, *ie*, to increase resilience of resources against natural disasters, *etc*. Hence, cloud

---

4 Peter Mell & Timothy Grance, *NIST Special Publication 800-145: The NIST Definition of Cloud Computing* (National Institute of Standards and Technology, 2011) at p 6 <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (accessed 24 January 2018).

5 *Privacy and Legal Issues in Cloud Computing* (Anne S Y Cheung & Rolf H Weber eds) (Edward Elgar Publishing, 2015) at p 14.

6 *Privacy and Legal Issues in Cloud Computing* (Anne S Y Cheung & Rolf H Weber eds) (Edward Elgar Publishing, 2015) at p 14.

computing often involves cross-border transfer of data (which often consists of personal data, depending on what the cloud is used for).

## III. Approaches under the Personal Data Protection Act to cloud computing

### *A. Data transfer restriction under the Personal Data Protection Act*

8 Under the Transfer Limitation Obligation, transborder data transfers are generally prohibited unless arrangements are made to ensure that a comparable standard of protection is afforded to protect the personal data.[7]

9 What is a "transfer" under the PDPA? There is no definition given in the PDPA, which leads to some interesting questions. For example, does the uploading of personal data on a webpage amount to a "transfer" of personal data? In the case of *Lindqvist*,[8] the European Court of Justice held that the loading of personal data onto an Internet site was not a "transfer" under the European Data Protection Directive[9] ("DPD"), notwithstanding that the page could be accessed from any country in the world. The court held that there was no transfer as the Internet pages did not send the personal information automatically to people who did not intentionally seek access to those pages. If the uploading of personal data on a webpage could be considered a "transfer", this may overextend the application of the data transfer restrictions of the DPD to all personal data that have been loaded onto the Internet.[10] While the position and decision taken has arguably left several unanswered questions,[11] the case does highlight the need to be practical in approaching the data transfer requirements, for otherwise, it

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

8 *Case C-101/01 Criminal proceedings against Bodil Lindqvist* [2003] I-12971.

9 Directive on the protection of individuals with regard to the processing of personal data and on free movement of such data (Directive 95/46/EC).

10 W Kuan Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens* (Edward Elgar Publishing, 2017).

11 W Kuan Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens* (Edward Elgar Publishing, 2017) at p 79.

may lend itself to illogical outcomes. In Singapore, there has been no case law on the interpretation of "transfer" under the PDPA.

10 The Transfer Limitation Obligation is embodied in s 26 of the PDPA along with its accompanying regulations under Pt III of the Personal Data Protection Regulations 2014[12] ("PDPR"). Under the PDPR, an organisation would need to satisfy two main requirements in order to ensure a "comparable standard of protection" ("Data Transfer Regulations"):

> (a) First, the organisation has to take appropriate steps to comply with the data protection provisions while the personal data are still in its possession or control.[13]
>
> (b) Second, the organisation has to take steps to ascertain and ensure that the recipient of the data transfer is bound by "legally enforceable obligations" to provide the comparable standard of protection.[14] Such "legally enforceable obligations" would include obligations that are imposed by law, contract, binding corporate rules or any other legally binding instrument.[15]

11 Based on the two requirements above, it is apparent that the drafters of the legislation intended to ensure a consistent protection over the personal data from the time before the transfer of the personal data to the time the data is safely in the hands of the recipient (and subsequently used by the recipient).

12 There are also instances under the PDPR where either or both of the two requirements are presumed to be satisfied. These include the instance where: (a) the data are in transit; (b) the personal data are publicly available; or (c) (in respect of the latter requirement) the transfer is required for the performance or conclusion of a contract.[16]

13 Even after the personal data have been transferred to the recipient, an organisation may still be liable or responsible for the protection of the personal data, as it may still be considered to be in "control" of the personal

12 S 362/2014.

13 Personal Data Protection Regulations 2014 (S 362/2014) reg 9(1)(*a*).

14 Personal Data Protection Regulations 2014 (S 362/2014) reg 9(1)(*b*).

15 Personal Data Protection Regulations 2014 (S 362/2014) reg 10.

16 Personal Data Protection Regulations 2014 (S 362/2014) reg 9(3).

data overseas, and hence, s 24 of the PDPA[17] would apply. Additionally, the transferring organisation ought to be familiar with the laws of the country in which the personal data are received as these laws may impose additional requirements relating to the transfer, or to the personal data entering into its jurisdiction.

14 Given that cloud computing often involves the transfer of personal data overseas, the question is what are the approaches available for companies to comply with the PDPA.

### *B. Various approaches under the Personal Data Protection Act*

15 Amongst the various ways in which organisations can comply with the PDPA for cross-border transfers, there is no one best solution or "silver bullet" for cloud computing.

#### *(1) Consent and presumptions*

16 Generally, the option of obtaining consent as the basis for transborder data transfers for cloud computing under reg 9(3)(*a*) of the PDPR is difficult in practice. While it may be good for one-off transfers of personal data overseas, it becomes impractical and unwieldy in respect of cloud computing where there is a need for multiple data transfers to multiple locations. The cloud service provider or the cloud user would have to know the details of the transfer beforehand, such as the purpose of the transfer, the recipients and countries to transfer to. Also, explaining the data flows in the cloud to the client may be difficult if the client is unfamiliar with cloud computing, or if the cloud setup is especially complicated. The individual can also withdraw consent at any time,[18] which may cause issues to the organisation if the personal data are already out of its hands, or if the personal data are in the midst of transfer and cannot be recovered easily.

---

17 Which 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.

18 Pursuant to s 16 of the Personal Data Protection Act 2012 (Act 26 of 2012).

17 Further, if the cloud user or cloud service provider handles the personal data of a large number of individuals, it may become burdensome to have to obtain their consent in making the data transfers.

18 In a recent public consultation paper,[19] the Personal Data Protection Commission ("PDPC") has sought views on the alternatives to consent, such as organisations providing notification where: (a) it is impractical to obtain consent; and (b) there is no appropriate adverse impact on the individuals from the collection, use or disclosure of personal data. This development may have an impact on the consent regime in the PDPA and, in turn, on the bases for data transfers under the PDPA.

19 As discussed above, the obtaining of consent is not the only legitimate basis for transferring data under the PDPR. The PDPR provides other bases, but in the context of cloud computing, it is hard to see how relevant or applicable the other bases are. For example, it is difficult to see how the use of cloud computing would be necessary to the performance of a contract,[20] if the contract itself does not stipulate that cloud computing will be used (and hence the organisation cannot rely on consent as well).

*(2) Contract*

20 An organisation can also enter into a contract with the recipient in order to comply with the Data Transfer Regulations. The contract should: (a) require the recipient to provide a comparable standard of protection; and (b) specify the countries and territories to which the personal data may be transferred under the contract.[21]

21 Following a study conducted by the WP29, it was found that contractual solutions are best suited to large international networks characterised by large quantities of repetitive data transfers of a similar nature.[22] Contracts are therefore somewhat useful for the purposes of cloud computing involving a fixed network.

---

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

20 Personal Data Protection Regulations 2014 (S 362/2014) reg 9(3)(*b*).

21 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(2).

22 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, "Working Document: Preliminary Views on the Use of

(*continued on next page*)

22 However, the contractual approach may pose a challenge to smaller businesses that have little bargaining power to negotiate for a contract beyond the standard terms of the counterparty, where such contracts may be suitable in addressing the counterparty's needs but not to comply with the PDPR.

23 Issues concerning private international law may also arise from the use of contracts for cross-border transfers. For example, if a contract is entered into by a cloud user and cloud service provider, and is enforced in a jurisdiction (in accordance with the private international laws of the country)[23] that does not recognise third-party rights, the data subject (*ie*, customer of the cloud user) may not have a contractual remedy against the cloud service provider for failing to comply with the contract to protect personal data.

24 As another example, if a foreign court which has seized jurisdiction over the contract has found the contract or a term of the contract to be illegal, how will this sit with the PDPA? Presumably, if the foreign court has found the contract to be invalid, then there is no valid contract under the PDPA and the transferor would be in breach of the Data Transfer Regulations. However, the answer may not be so clear if the foreign court finds that the contract is still valid notwithstanding the illegal term, but the illegal term is needed to give effect to a comparable protection under the PDPA.[24]

25 Also, the very essence of cloud computing is that the data and equipment are not tied to or associated with any particular jurisdiction, but are located in the "cloud". It may thus be a difficult exercise to determine the country/jurisdiction whose laws govern the transfer that was carried out, given the ephemeral nature in which the data are transferred across countries. That said, in terms of contracts, the law governing a contract is

---

Contractual Provisions in the Context of Transfer of Personal Data to Third Countries" <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp9_en.pdf> (accessed 19 December 2017).

23 There are three stages to determine the proper law of a contract: *Pacific Recreation Ptd Ltd v S Y Technology Inc* [2008] 2 SLR(R) 491 and *Peh Teck Quee v Bayerische Landesbank Girozentrale* [1999] 3 SLR(R) 842.

24 Under the blue pencil doctrine: *Thorsten Nordenfelt v Maxim Nordenfelt Guns and Ammunition Co Ltd* [1894] AC 535.

usually determined by the choice of law clause, and thus an organisation seeking to bring some certainty on the applicable law to the data transfer contract could possibly do so by incorporating the appropriate choice of law clause.

26 Separately, it should be highlighted that the PDPC has recently provided some sample clauses on its website,[25] including on data transfers, which may be a useful guide for organisations on what to include in a data transfer contract.[26]

### *(3) Binding Corporate Rules*

27 Binding Corporate Rules ("BCRs") have been described as codes of conduct dealing with the international transfer of personal data within the same corporate group (or related companies) at a multinational level.[27] Under the PDPR, companies are considered to be "related" if either company "controls" the other, or if a common person controls the companies.[28] There is no definition of "control" in the PDPA, but it would clearly include control by way of shareholding – *ie*, a holding company and its subsidiaries. By taking a broad interpretation of the word "control", it may also apply to a situation where a person is a sole director of two separate companies, and has decision-making powers over the operations of the companies, but does not have majority shareholding over the companies.[29]

28 However, because there is a need to establish a direct or indirect relationship of "control" between the transferring organisation and recipient, BCRs may not apply to an organisation-data intermediary relationship, where the data intermediary is an independent contractor of

---

25 *Eg*, <https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-on-dp-clauses-for-agreements-related-to-processing-of-personal-data-v1-0-(200716).pdf?sfvrsn=3> (accessed 19 December 2017).

26 Organisations would need to ensure that they modify or adapt the clauses to suit their needs and the requirements for data transfers under the Personal Data Protection Act 2012 (Act 26 of 2012).

27 Christopher Millard, *Cloud Computing Law* (Oxford: Oxford University Press, 2013) at p 267.

28 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(4).

29 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(4).

the organisation. If such an interpretation is to be taken of a "related"[30] organisation under the PDPR, the PDPR will appear more limited than the DPD, which have introduced processor BCRs[31] as a means for data transfer. Processor BCRs allow transfers from a data controller to an external processor, such as a cloud service provider. BCRs under the PDPR would then only be useful for intra-corporate group cloud computing, as opposed to inter-corporate cloud computing.

29 One of the advantages of using BCRs is that BCRs allow for ongoing data transfers, and do not operate on a one-off basis as in the case of consent, for example. This would be useful for cloud computing where the group of companies expect multiple cross-border transfers to be made amongst themselves on an ongoing basis. Additionally, BCRs promote accountability amongst the companies as they require the group of companies to organise and align their process and practices around certain data protection obligations and principles.

30 The main disadvantage of using BCRs for cloud computing is that they only allow data transfers amongst related companies. This limits the number of organisations that can participate in the cloud computing set-up, and affects the size and scalability of the cloud computing service. Additionally, BCRs may not be useful if the group structure regularly changes, thereby requiring BCRs to be amended frequently.

### *(4) Technical solutions*

31 Although not expressly provided for in the PDPA, another solution for transferring data overseas could be a technical one – *eg*, anonymising or encrypting data.

32 The anonymisation guidelines[32] issued by the PDPC provides that the data protection provisions ("DP Provisions") of the PDPA would not apply if effective anonymisation techniques and risk mitigation controls have been applied and there is no serious possibility that the data can be used to

30 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(4).

31 See, for example, the processor Binding Corporate Rules that Salesforce had managed to get approval for.

32 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at para 3.3.

identify an individual. In other words, by applying anonymisation techniques to the personal data, the anonymised data are no longer personal data that are subject to the PDPA. The anonymisation guidelines also provides that even in such circumstances where within the organisation, there is other information that can re-identify the individual (*eg*, a decryption key),[33] but the organisation has ensured that there are barriers to access to such information, the DP Provisions would not apply.

33 Similarly, it is arguable that the DP Provisions do not apply to encrypted data which cannot identify an individual. If this argument is accepted, then the encryption of personal data may be one similar way of transferring personal data. For example, a small to medium-sized enterprise ("SME") looking to store its clients' personal data (such as their photos or contact details) in a cloud service in another country can do so by encrypting data securely before uploading them to the cloud. When there is a need to use the data, the organisation can download the encrypted data to its local computer for decryption. However, this approach may limit the usefulness of the data for *real-time* processing, if conventional encryption is used.[34]

34 *Homomorphic encryption* is a more advanced type of encryption which makes it possible to directly process *encrypted* data. Current research efforts have largely only been able to achieve encryption that is partially homomorphic, meaning that only limited types of computational operations and processing are possible, instead of fully homomorphic, where arbitrary computation is possible.[35] If fully homomorphic encryption were to be achieved, the implications would be ideal and very desirable, because data would remain encrypted while stored in the cloud, yet can be processed and used at the same time by authorised cloud users.[36] This

33 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 28 March 2017) at paras 3.37–3.42.

34 C Mitchell, "Privacy, Compliance and the Cloud" in *Guide to Security Assurance for Cloud Computing* (S Y Zhu, R Hill & M Trovati eds) (Springer, 2015) at para 1.1.

35 J Aldermann, J Crampton & K M Martin, "Cryptographic Tools for Cloud Environments" in *Guide to Security Assurance for Cloud Computing* (S Y Zhu, R Hill & M Trovati eds) (Springer, 2015) at para 3.4.1.2.

36 Hence, the data protection provisions likely still apply to the authorised cloud user.

means that even if unauthorised parties were to seize the data, they would not be able to access the original personal data. Additionally, the cloud user which processes and uses the data as personal data would likely be subject to the DP Provisions of the PDPA, and would have to comply with their obligations therein (such as ensuring that reasonable security arrangements are made to protect the personal data).

35 *Bit splitting*[37] is another example of a technology that could address the security of personal data in the cloud. With bit splitting, data are split into fragments and stored across multiple cloud storage services in different geographical locations. The design is such that the data are only complete when recombined; data fragments stored at a single location are incomplete, or even unrecognisable. Again, this means that even if unauthorised parties were to seize the data from a single location, they would not be able to access the original personal data (at least not in the complete form).

36 There are potential difficulties associated with the use of technical solutions. These include:

(a) Additional resources required, due to decreased performance. For example, the processing power required to process *homomorphically* encrypted data is currently still too vast for homomorphic encryption to be deployed for general purposes.[38]

(b) Some of the technologies that could potentially be useful are not matured yet, and are still undergoing active research and development.

(c) Technical solutions may be more applicable for IaaS implementations only, due to the limited control that the cloud user is given over the system and application for SaaS and PaaS implementations.

37 Although the use of technical solutions may not be the panacea for all cloud computing data transfers, it does offer an option for SMEs as it may be a simpler approach to adopt than having to execute a contract (for which

37 A Gordon, *The Official (ISC)2 Guide to the CCSP CBK* (Sybex, 2nd Ed, 2016) at p 106.

38 C Mitchell, "Privacy, Compliance and the Cloud" in *Guide to Security Assurance for Cloud Computing* (S Y Zhu, R Hill & M Trovati eds) (Springer, 2015) at para 1.1.

an SME may not have any bargaining power or the expertise) or to obtain consent for every transfer made.

*(5) Law*

38 Following the Court of Justice of the European Union's decision in *Maximillian Schrems v Data Protection Commissioner*[39] ("*Schrems*"), the 15-year old Safe Harbor programme was deemed invalid. Underscoring the decision is the finding that the Safe Harbor programme did not provide an "adequate" protection for European Union ("EU") data subjects because, amongst other things, there was no finding of the appropriate safeguards to protect the rights and data of EU data subjects, where such interference may be for legitimate objectives (*eg*, national security).[40]

39 The Safe Harbor programme has now been replaced by the Privacy Shield. The Privacy Shield imposes "stronger obligations on companies in the US to protect the personal data of individuals and stronger monitoring and enforcement by the US Department of Commerce ('DOC') and Federal Trade Commission ('FTC')".[41] It should be noted that there are ongoing legal challenges made before the European courts against the Privacy Shield,[42] and given the new rules in force under the EU General Data Protection Regulation ("GDPR"), the future of the Privacy Shield is unclear.

40 *Shrems* is important in highlighting the difficulties in relying on the "laws" of another country for adequacy of protection. If there can be disagreement on whether the Safe Harbor or Privacy Shield can afford an equivalent protection[43] proffered by EU laws, it may be difficult for organisations to find that a country's "laws" offer a comparable standard of

39 C-362/14 (6 October 2015).

40 *Maximillian Schrems v Data Protection Commissioner* (C-362/14) (6 October 2015) at [88].

41 "European Commission – Fact Sheet – EU-U.S. Privacy Shield: Frequently Asked Questions" <http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm> (accessed 19 December 2017).

42 Rosemary Jay, *Guide to the General Data Protection Regulation* (UK: Sweet & Maxwell, 2017) at para 8-006.

43 *Maximillian Schrems v Data Protection Commissioner* (C-362/14) (6 October 2015) at [73].

protection under reg 10(1)(*a*) of the PDPR. Consequently, the reliance on "laws" as a legal basis under the PDPR for data transfer may not be suitable for cloud computing.

41 Nevertheless, there are some positive developments in this area. Recently, Singapore has joined the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR") and Privacy Recognition for Processors ("PRP") Systems.[44] The APEC CBPR System is a voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies.[45] The APEC CBPR System applies to data controllers, which include organisations that control the collection, holding, processing or use of data. The PRP System applies to data processors, which include organisations that process data on behalf of other organisations at their instruction.[46] Companies would have to undergo certification in order to participate in the schemes.

42 One of the stated purposes of the APEC CBPR is to facilitate the transfer of personal information across participating APEC economies in a manner in which individuals may trust that the privacy of their personal information is protected.[47] If, ultimately, the APEC CBPR allows for the free flow of transfer of personal data amongst CBPR-certified companies in participating economies, this is likely to make it easier for the development of cloud computing services across the participating economies in the APEC region. Presumably, the PDPA would then allow such transfers to be

---

44 Announcement by the Ministry for Communications and Information available at <https://www.mci.gov.sg/budget-workplan/cos2018/modules/articles/for%20our%20workers%20and%20businesses/apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems> (accessed 10 March 2018).

45 "About the APEC CBPR system" <http://cbprs.org/GeneralPages/About.aspx> (accessed 10 March 2018).

46 Factsheet available at <https://www.mci.gov.sg/budget-workplan/cos2018/modules/articles/for%20our%20workers%20and%20businesses/apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems> (accessed 10 March 2018).

47 *APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines* <https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf> (accessed 10 March 2018).

made provided that they comply with the requirements of the APEC CBPR.

43 Adoption of the APEC CBPR could lead to the development and promotion of regional cloud computing services in the region.[48] Such regional clouds would be a welcomed initiative in Singapore as it ensures a certain level of data protection in the APEC countries, while making it easy for companies to take on cloud computing services.

*(6) Other option – Exemption under section 26(2) of the Personal Data Protection Act*

44 One final option is for companies to seek an exemption from the PDPC to the Transfer Limitation Obligation under s 26(2) of the PDPA. Such exemptions are likely to be rare, and granted only in exceptional circumstances where the organisation demonstrates that it is unable to comply with the Transfer Limitation Obligation. Further, the granting of exemptions is more likely suitable for one-time transfers. It is therefore unlikely to be suitable for cloud computing unless a one-time transfer of personal data (for testing or otherwise) is needed by the organisation.

## IV. Way forward

45 Given the growing importance of cloud computing to businesses and consumers, there may be a need to look at how to improve this area of law on data transfers.

46 The first suggestion is to move away from the focus of comparing the laws of a country to find a "comparable standard of protection". The problem with using a territory's laws as the litmus test of the "adequacy" of protection is that it may not be an accurate measurement of the actual security that is protecting the personal data. Having strict laws does not necessarily mean that the personal data are any safer – just as a "weaker" law does not mean the personal data are unprotected. Instead, more emphasis should be placed on the accountability of the organisation in protecting the personal data transferred overseas. So long as companies are accountable for

48 This is not new – for example, the Cisco Meraki Cloud has its data centres located exclusively in the European Economic Area.

the protection, they should be free to decide on how to structure the transfer and to protect the personal data. This means, for example, being less stringent on requirements such as the requirement to spell out the list of countries in a BCR document[49] – that ought not to be fatal in preventing transfers from being made.

47 Another suggestion is for the PDPA to expressly recognise approved codes of conduct or certification as a means for data transfer, similar to what the EU GDPR has done. Under the GDPR, codes of conduct and certification mechanisms can be used to establish adequacy of transfers, provided that there are binding and enforceable commitments to apply the appropriate data protection safeguards.[50] Allowing approved codes of conduct or certification as a means for data transfer not only gives organisations more avenues for data transfers, it also encourages organisations to align their standards and adopt good data protection practices. Since the PDPR already allows for international data transfers under a "legally binding instrument",[51] this could be extended to include such instruments as binding codes of conduct or certification. In Singapore, a new certification mark is being developed,[52] and the recognition of codes of conduct and certification should nicely dovetail into the overall objective of this certification programme.

## V. Conclusion

48 There are lofty goals for Singapore to be a global and regional cloud computing hub.[53] Indeed, Singapore has all the makings to be a global data hub on the digital data highway – it is stable, reliable and business-friendly,

---

49 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(3)(*b*)(ii).

50 Rosemary Jay, *Guide to the General Data Protection Regulation* (UK: Sweet & Maxwell, 2017) at para 8-032.

51 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(1)(*d*).

52 See <https://www.pdpc.gov.sg/docs/default-source/media/Seminar-2017-PR/pdps2017-media-release---(260717).pdf?sfvrsn=0> (accessed 19 December 2017).

53 Infocomm Development Authority of Singapore Fact Sheet, "A New Paradigm in Cloud Computing" <https://www.imda.gov.sg/-/media/imda/files/inner/about-us/newsroom/speeches/2013/1505_cloudasia2013/cloudcomputingfactsheet.pdf?la=en> (accessed 19 December 2017).

a truly safe harbour for data. In order to meet these aspirations, it is important that the legal landscape facilitates and promotes cross-border transfers, and to take a rational approach, that is, one that balances the interests of protecting personal data whilst ensuring that businesses are not inhibited from transferring data overseas.

49 The authors believe that there are several approaches companies can adopt now under the current PDPA to support their cloud computing needs, as mentioned above. Overall, the PDPA does seek to facilitate data transfers overseas and offers the flexibility in choosing the protection mechanisms in transferring data. This should be good news for businesses looking to use cloud computing. However, protecting personal data should not be viewed simply as a compliance issue to a business, but regarded as a core business value offered to its customers. Therefore, it makes good business sense to fully comply with the Transfer Limitation Obligation under the PDPA. That should be the mission to which a company strives towards.

# REGULATION OF BIOMETRIC DATA UNDER THE PERSONAL DATA PROTECTION ACT*

**Gilbert LEONG**†
*LLB (National University of Singapore), LLM (University College London); Advocate and Solicitor (Singapore)*

**FOO Maw Jiun**‡
*LLB (National University of Singapore); Advocate and Solicitor (Singapore)*

**Desmond CHEW**§
*LLB (Singapore Management University); Advocate and Solicitor (Singapore)*

## I. Introduction

1 In Singapore's march towards becoming a smart nation, there is an increasing prevalence of the collection, use and disclosure of biometric data. Multiple touchpoints for the use of biometric data can now be found across Singapore, from facial and thumbprint recognition for immigration clearance at Changi Airport's Terminal 4, to the use of primary school students' fingerprints to pay at their schools' tuckshops,[1] to the use of voice technologies to perform secured financial transactions.[2] This necessitates a

---

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

† Senior Partner, Dentons Rodyk & Davidson LLP, IP & Technology Practice Group. Gilbert is very active in the field of data privacy/protection matters, having acted for large financial institutions, healthcare providers and industrial companies. He has also written and spoken widely on the area.

‡ Partner, Dentons Rodyk & Davidson LLP, IP & Technology Practice Group.

§ Associate, Dentons Rodyk & Davidson LLP, IP & Technology Practice Group.

1 "Biometric Payment System to be an Option in Schools in 2018" *Channel NewsAsia* (21 August 2017).

2 Fintechnews Singapore, "OCBC Bank Singapore Goes Voice Recognition Technology for Business Banking Mobile Solutions" (4 October 2017) <http://fintechnews.sg/12515/mobile-payment/ocbc-bank-leads-charge-asia-

(*continued on next page*)

more rigorous scrutiny and consideration of how organisations handle such data, and whether our existing data protection laws are sufficient.

2 The collection and exploitation of biometric data raises privacy concerns that transcend beyond those associated with traditional types of personal data (*eg*, names, e-mail addresses and mobile numbers). Biometric data usually take the form of a ubiquitous identifier that cannot be modified or replaced by an individual (*eg*, fingerprints, palm veins, facial recognition and iris recognition). As such, biometric data are often used for the most important transactions where there is a need for identity verification (*eg*, financial transactions). The consequences of any misuse or abuse of biometric data (such as identity theft) can be dire.

3 Accordingly, the authors suggest that the Personal Data Protection Act 2012[3] ("PDPA") should be amended to account for the specific nuances of biometric data, and ensure that organisations abide by baseline standards when handling biometric data. The Personal Data Protection Commission ("PDPC") may also consider requiring organisations wishing to handle biometric data, to register with the PDPC, and abide by such baseline standards.

## II. WHAT IS BIOMETRIC DATA

### *A. Defining biometric data*

4 There is no universal consensus on the definition of "biometric data". The *Merriam-Webster Dictionary* defines biometry simply as the "statistical analysis of biological observations and phenomena". Across jurisdictions which regulate biometric data, there are also different approaches taken, and different definitions of biometric data. While there is a general consensus that inherent characteristics of an individual (*eg*, retina pattern and fingerprints) constitute biometric data, certain jurisdictions have also considered behavioural data (*eg*, a person's gait and speech pattern) to be biometric data as well:

---

using-voice-recognition-technology-business-banking-mobile-solutions> (accessed 2 January 2018).

3 Act 26 of 2012.

(a) The European Union ("EU") in its General Data Protection Regulation[4] ("GDPR") defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images".

(b) In the US, there is no federal law for privacy protection. States such as Illinois and Texas have taken the lead in biometric data protection. Both states have defined a biometric identifier as a "retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry".[5] Unlike the EU, these states have chosen to only regard biometric data as that which is inherent in an individual (*ie*, physical or physiological characteristics of a natural person).

(c) Hong Kong has not defined the term "biometric data" in its privacy legislation. Instead, Hong Kong's Office of the Privacy Commissioner for Personal Data ("PCPD") has issued guidance notes to explain the circumstances in which its privacy legislation will regulate biometric data, and what types of data will constitute "biometric data". These notes have defined biometric data as both: (i) "physiological data with which individuals are born", and (ii) "behavioural data which is characteristics developed by an individual after birth", a position similar to that of the EU.[6]

5 Biometric data are not expressly provided for, or defined under Singapore's PDPA. Our PDPC recognises that biometric data do fall within the definition of "personal data" under the PDPA, as such data can by themselves identify an individual (*eg*, face geometry, fingerprint, iris image and DNA profile).[7] However, whether this definition includes behavioural data is less clear (*eg*, unique gestures that an individual frequently makes).

---

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

5 See the, Biometric Information Privacy Act (740 ILCS 14/1) (2008) (Illinois) and the Business and Commerce Code (Title 11 Personal Identity Information) (Texas).

6 Office of the Privacy Commissioner for Personal Data, Hong Kong, *Guidance on the Collection and Use of Biometric Data* (July 2015).

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

The authors have previously argued that the PDPA does not limit the forms and manifestation of data that count as "personal data".[8] However, in analysing behavioural data, a case-by-case inquiry is required to determine whether such data can personally identify an individual (whether by themselves or with other data).

### *B. Uses of biometric data*

6 Biometric data may be used in a number of different settings but in general it is observed that they are used for the following:

> (a) **identification**: capturing and enrolling the individual's biometric data into a database for the data to be linked to a template for future identity matching;[9]
>
> (b) **authentication**: ensuring that the individual's presented credential matches the samples provided to the organisation;[10] and
>
> (c) **authorisation**: allowing an individual to provide consent for the provision of goods and/or services through the provision of personal data.[11]

7 In order to achieve the above, an individual will first need to provide his biometric data (*eg*, fingerprints) to an organisation for enrolment into the organisation's database. At this stage, the biometric data serve no purpose yet as the biometric data are not associated with any individual. However, the organisation will subsequently extract the biometric data to

---

8 Gilbert Leong, Foo Maw Jiun & Kenneth Fok, "Protecting the Right of Publicity under the Personal Data Protection Act" [2017] PDP Digest 293 at para 17.

9 InfoSec Institute, "Biometrics: Today's Choice for the Future of Authentication" <http://resources.infosecinstitute.com/biometrics-todays-choice-future-authentication/#gref> (accessed 1 January 2018).

10 InfoSec Institute, "Biometrics: Today's Choice for the Future of Authentication" <http://resources.infosecinstitute.com/biometrics-todays-choice-future-authentication/#gref> (accessed 1 January 2018).

11 Annemarie Sprokkereef, "Data Protection and the Use of Biometric Data in the EU" in *The Future of Identity in the Information Society* (S Fischer-Hübner *et al* eds) (IFIP, Book 262) (Springer, 2008) at pp 277–284.

create a biometric template, which is then associated with an individual for future identification purposes.[12]

8 The advantages of biometric data are self-evident. From the end-user's perspective, it presents a more secured and convenient way of performing transactions with governments and organisations.[13] The only individual authorised to perform the transaction is the individual who possesses and presents the biometric data. Biometric data can also serve as an effective replacement for password authentication, thereby reducing costs and inconveniences associated with password replacements and issuance of company credentials. These advantages, however, must be considered in the light of potential issues, such as the protection and retention of biometric data.

## III. Risks associated with biometric data

### *A. Collection of biometric data*

9 The promise of convenience has often been undermined by technological challenges faced by organisations in the collection and use of biometric data. First, biometric systems may not necessarily recognise the end-user's biometric data for a variety of reasons. For instance, it is commonplace that ambient background noises affect the authentication of an individual's voice, thereby affecting the functionality of the system.[14] Such inconveniences impair the end-users' trust in biometric systems.

10 Second, health and age issues impact the collection of biometric data by organisations. Dermatologists have shared that factors such as eczema,

12 Mary Rundle & Chris Conley, *Ethical Implications of Emerging Technologies: A Survey* (2007) <http://unesdoc.unesco.org/images/0014/001499/149992e.pdf> (accessed 2 January 2018).

13 A Rjeily & C Jacco, "Passwords are Terrible, but Will Biometrics Be Any Better?" *Harvard Business Review* (11 May 2017).

14 InfoSec Institute, "Biometrics: Today's Choice for the Future of Authentication" <http://resources.infosecinstitute.com/biometrics-todays-choice-future-authentication/#gref> (accessed 1 January 2018).

infections and age can cause a complete or partial loss of fingerprints.[15] In 2017, three in 100 people continue to have problems with having their fingerprints scanned at Singapore's automated immigration clearance gates.[16] For organisations, this means that to improve on the collection of biometric data, biometric systems may have to be periodically updated to stay relevant and accurate.

11 Third, biometric systems are not entirely foolproof, and are also vulnerable to tampering. For instance, facial recognition features on smartphones may be fooled by using another individual's photo,[17] which raises serious concerns about reliability and security. Further, facial recognition systems presently used to identify suspects are not infallible; they are reported to have a 15% chance of error.[18] Notably, such challenges are likely to persist for the foreseeable future.

### *B. Problematic uses of biometric data*

12 Unlike other types of personal data (*eg*, mobile numbers), biometric data are immutable. Once compromised, the damage and harm to the individual may be permanent. The form of damage goes beyond receiving unsolicited marketing messages; the individual suffers risks of impersonation, fraud and identity theft, all of which may cause serious personal harm and monetary losses.

13 Even where biometric data are initially collected for a specific purpose, it has been observed that there is a tendency for organisations to use the data for other unintended or unauthorised purposes. The Organisation for Economic Co-operation and Development ("OECD") has termed this as a "function creep", having observed that finger scans collected for a particular

15 InfoSec Institute, "Biometrics: Today's Choice for the Future of Authentication" <http://resources.infosecinstitute.com/biometrics-todays-choice-future-authentication/#gref> (accessed 1 January 2018).

16 Toh Wen Li, "Faint Fingerprints an Issue for some at Border Scans" *The Straits Times* (2 October 2017).

17 Steve Kovach, "Samsung's Galaxy S8 Facial Recognition Feature Can Be Fooled With a Photo" *Business Insider* (31 March 2017).

18 Simon Denyer, "Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance" *The Washington Post* (7 January 2018).

purpose (*eg*, guarding against welfare fraud) could be subsequently used for other unrelated purposes.[19]

14 Biometric data can also be combined with other available information about an individual (*eg*, on social networking platforms) to form a comprehensive profile, such that the individual's identity itself can be commercialised (or manipulated). The OECD has observed that AC Nielsen has patented a facial recognition system that captures individuals' facial recognition data for the purpose of tracking shoppers' buying habits, thereby facilitating targeted marketing.[20]

15 Despite these challenges associated with biometric data, it is projected that there will be further significant benefits to be reaped, as biometric technologies develop greater sophistication to harness such data. The key question then is how these challenges and risks can be addressed through regulation, including whether and how higher data protection standards may be set for biometric data (as compared to traditional types of personal data). Before considering the Singapore position, it is helpful to first consider how foreign jurisdictions have enacted specific laws dealing with biometric data, and how these laws have been applied.

## IV. Foreign jurisdictions and their experiences with biometric data

### *A. State of Illinois, United States of America*

16 In Illinois, the Biometric Information Privacy Act[21] ("BIPA") provides that no private entity may obtain a person's biometric information, unless it informs the individual in writing that his biometric identifier is being

19 Working Party on Information Security and Privacy, *Biometric-Based Technologies* (30 June 2004) <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)2/FINAL&docLanguage=En> at p 12 (accessed 2 January 2018).

20 Working Party on Information Security and Privacy, *Biometric-Based Technologies* (30 June 2004) <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)2/FINAL&docLanguage=En> at p 13 (accessed 2 January 2018).

21 740 ILCS 14/1 (2008).

collected, state the specific purpose and length of term for which the biometric information is being stored and used, and receives a written release by the individual.[22]

17 However, the BIPA does not prescribe a baseline standard for the storage and security arrangements of biometric information. Instead, private entities are only obliged to protect biometric identifiers on a reasonable standard of care basis, commensurate with their industry and in a manner that is the same as or more protective than treating confidential information.[23] Clearly, the BIPA is cognisant of the highly sensitive nature of biometric information.

18 The BIPA also requires private entities to establish a retention schedule and guidelines for permanently destroying biometric identifiers. For instance, private entities must destroy the biometric information when the initial purpose of collecting such information has been satisfied, or within three years of the individual's last interaction with the entity, whichever occurs first.[24]

### *B. European Union*

19 In the EU, the GDPR, which comes into force on 25 May 2018, reiterates the need for effective data protection impact assessments, especially where biometric data are involved.[25] Article 9(1) of the GDPR specifically prohibits the processing of biometric data for the purposes of identification, unless any of the exceptions under Art 9(2) apply (*eg*, the subject has given explicit consent to the specified purposes of processing his biometric data).

20 Article 9(4) of the GDPR further permits Member States in the EU to maintain or introduce further conditions with regard to the processing of biometric data, provided that these conditions should be balanced against the possible hampering of the free flow of personal data within the EU.[26]

---

22 Biometric Information Privacy Act (740 ILCS 14/1) (2008) §15(b).

23 Biometric Information Privacy Act (740 ILCS 14/1) (2008) §15(e).

24 Biometric Information Privacy Act (740 ILCS 14/1) (2008) §15(a).

25 European Union General Data Protection Regulation Council Text at p 41.

26 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 at para 53.

### C. *Hong Kong*

21 Although biometric data is not defined in Hong Kong's privacy legislation, the Hong Kong PCPD has issued a guidance note[27] ("HKGN") which advises data users on: (a) the need for caution in handling sensitive biometric data; (b) the justifications for collection and use of biometric data; (c) risk minimisation techniques in biometric data collection; (d) the need for a privacy impact assessment; (e) providing free and informed choice in collecting biometric data; and (f) privacy requirements for dealing with biometric data collected. The guidance also addresses how data users should take precautions that vary according to the sensitivity of the biometric data concerned.

## V. Biometric data in Singapore context

### A. *Privacy concerns in public sector*

22 With Singapore's march towards becoming a smart nation, it is inevitable that the Government and its public agencies will be amongst the largest collectors and users of biometric data, *eg*, by collecting such data through the National Registration Act.[28] The elephant in the room is, of course, that the PDPA does not apply to the Government and its public agencies.[29] However, it would be remiss of the authors not to discuss privacy concerns in the public sector context given its extensive collection and use (though mainly in the law and order domain) of biometric data.

23 Minister for Information, Communications and the Arts, Dr Yaacob Ibrahim, has stated that the PDPA will not cover the public sector as "the public sector already has its own set of data protection rules that all public officers must comply with". In addition, Singapore has also recently passed the Public Sector (Governance) Act 2018.[30] This new Act will come into

27 Hong Kong, PCPD Guidance on the Collection and Use of Biometric Data <https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf> (accessed 26 December 2017).

28 Cap 201, 1992 Rev Ed.

29 Simon Chesterman, "Privacy and Our Digital Selves" *The Straits Times* (2 September 2017).

30 Act 5 of 2018.

force on 1 April 2018 and will make it an offence for individuals within public agencies to disclose unauthorised information to another party, or take steps to re-identify anonymised information.[31]

24 Clearly, while there may be legislation to address the unauthorised disclosure of information by civil servants, it is unclear how public agencies will handle biometric data, or whether consent of individuals will be obtained, prior to the sharing of biometric data amongst agencies or enlarging the scope of use of collected biometric data. To illustrate this point, Chongqing commenced an ambitious project to connect security cameras at public spaces, with private cameras in buildings, into "one nationwide surveillance and data-sharing platform".[32] Facial recognition and artificial intelligence will be used to co-ordinate public agency services, such as tracking suspects and predicting crime. However, it must be noted that this project can also be used simultaneously to track dissidents. In the absence of any legislation regulating the use of biometric information by the public sector, it is unclear whether such "functional creep" of biometric data can happen in the Singapore context.

### *B. Limitations of the Personal Data Protection Act*

25 The PDPA defines "personal data" as data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.[33] Although biometric data are not expressly mentioned in the PDPA, there is little doubt that biometric data fall within the confines of "personal data". Accordingly, the provisions in the PDPA as well as the PDPC's general guidance in relation to personal data apply to biometric data. The issue

31 Sections 7 and 8 of the Public Sector (Governance) Act 2018 (Act 5 of 2018). Pursuant to s 2(1) of the Act, "information" has been defined to include (a) any facts, statistics, instructions, concept or other data in a form that is capable of being communicated, analysed or processed (whether by an individual or a computer or other automated methods); and (b) data sets. The expansive definition of "information" appears to be sufficiently broad to cover biometric data.

32 Simon Denyer, "Beijing bets on facial recognition in a big drive for total surveillance" *The Washington Post* (7 January 2018).

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

then is whether specific provisions or guidance are needed for the collection, protection, retention and destruction of biometric data by organisations, as opposed to the current regime under the PDPA relating to delimiting the collection, use and disclosure of personal data.

26 It is observed that the general provisions of the PDPA already reflect certain protective measures over biometric data which can be found in other jurisdictions:

(a) The PDPA requires consent to be obtained from the individual for the collection, use and disclosure of personal data, and these purposes must be notified to the individual (in line with the BIPA and the HKGN).[34]

(b) The PDPA also contains provisions concerning the retention and protection of personal data (in line with the GDPR and the HKGN).[35]

27 However, there are challenges in applying the present PDPA framework to biometric data:

(a) First, while the PDPA prescribes that organisations should put in place reasonable security arrangements to protect personal data, there is no consensus as to what these reasonable standards would be when it comes to biometric data. The PDPC's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[36] states that there is no "one-size-fits-all" solution when it comes to complying with the protection obligation. It obliges organisations to consider the nature of the data involved. Nonetheless, it is unclear whether biometric data ought to be accorded greater attention as opposed to traditional forms of personal data. Given the inherent uncertainty as to what "reasonable" might mean in relation to the collection and protection of biometric data, organisations may end up spending significantly more (*eg*, so as to meet the high watermark ISO/IEC 24745:2011) than what may be required or indeed intended under the "reasonable standard of protection" rubric.

---

34 See, *eg*, ss 13 and 20 of the Personal Data Protection Act 2012 (Act 26 of 2012).

35 See, *eg*, ss 24 and 25 of the Personal Data Protection Act 2012 (Act 26 of 2012).

36 Revised 27 July 2017.

(b) Second, new developments to the PDPA may not have sufficient regard to the nuances of biometric data. The PDPC is now considering amending the PDPA to allow organisations to notify individuals that they would be collecting, using and disclosing personal data, where the purpose of the collection, use or disclosure of personal data is not expected to have any adverse impact on the individual.[37]

Suppose a shopping mall records CCTV images of its shoppers, and places a general notification on its website or social media platform(s) that shoppers' images will be recorded for surveillance and data analytics purposes. At a later stage, the mall decides to collect and use the CCTV images to identify shopping patterns of its shoppers. The mall then sends out a second notification to its shoppers that their personal data will now be used for an additional purpose such that it allows the mall to tailor advertisements within the premises to target users' shopping habits. It is unclear whether (i) the purpose of allowing malls to provide tailored advertisements through the notification process will not be considered to have any adverse impact on individuals; and (ii) the issuance of a second notification which modifies the original purposes for which the personal data were first obtained will amount to having an adverse impact on the individuals.

### *C. Recommendations*

28 Given the immutable nature of biometric data and the grave risks associated therein, there is a corresponding need for biometric data-specific provisions pertaining to the collection, protection, retention and destruction of such data in the PDPA (*eg*, those found in the BIPA and GDPR). The present situation is unsatisfactory; the PDPA requires "reasonable" security arrangements to protect personal data, but does not provide guidelines on what exactly constitutes such reasonable arrangements. Organisations are thus left to determine for themselves as to what constitutes reasonable security arrangements. Often, this determination is largely dependent on cost considerations and the operational use of the

37 Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy" (issued 2 February 2018).

data, as opposed to what should be reasonable in the light of the sensitive nature of biometric data.

29 The benefits of having clear lines in the legislation are numerous: organisations would know what the specific rules concerning the collection, protection, retention and destruction of biometric data are, and an infraction of such rules would be obvious. The difficulty with such a proposal is of course the question as to what the appropriate rules to govern biometric data are. By setting a clear line for biometric data, there is a risk that such standards may not be appropriate for all circumstances concerning biometric data.

30 In order to mitigate such challenges, the authors would suggest that the present amorphous concepts found in the PDPA (*eg*, reasonable security arrangements) be retained, with the introduction of minimum standards with respect to biometric data. Such minimum standards that can be legislated include:

> (a) adopting encryption technologies when collecting and processing biometric data;
> (b) destroying the biometric data once the initial purpose has been fulfilled, or within three years' of the individual's last interaction with the organisation (mirroring the BIPA); and
> (c) general restrictions on the selling or trading of biometric information for profit (or otherwise), or using biometric data outside of identification purposes (*eg*, found in the BIPA and GDPR).

31 The authors have also considered placing such standards in the PDPC's advisory guidelines. However, such guidelines are advisory in nature and are not legally binding on the PDPC.[38] In any event, these standards (*eg*, encryption technologies) are already expected by the PDPC as necessary precautions for sensitive personal data, and these standards merely enshrine the security standards expected of organisations.[39]

32 Conversely, it may be argued that such baseline standards impose unnecessary compliance costs on organisations, and impede technological innovations. However, such arguments are overstated. If an organisation is

---

38 Personal Data Protection Commission, *Introduction to the Guidelines* at para 3.1.

39 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [26].

sophisticated enough to deploy biometric systems, surely it ought to be equally capable of deploying security arrangements that can meet (or exceed) the prescriptive standards of protection. Further, reckless use or storage of biometric data should most definitely be discouraged.

33 It might be ideal to require organisations to register with the PDPC if they wish to implement biometric systems. This allows the PDPC to have oversight of the organisations' treatment of biometric data, and impose codes of practice on them (*ie*, as presently imposed for media and telecommunications licences under the Info-communications Media Development Authority). This scheme further promotes the vision of a smart nation, as it encourages the responsible handling of biometric data by organisations. If an organisation breaches such codes of practice, the PDPC may revoke their registration, and take swift steps to contain the breach.

## VI. Concluding thoughts

34 There is no clear solution as to how jurisdictions can effectively treat or regulate biometric data. What is clear, however, is that there ought to be more regulation, given that the risks associated with such data are likely to become more pervasive and multifaceted, as more organisations use biometric technologies. Given the gravity of privacy concerns associated with biometric data, and the immutability of such data, it is now an opportune time for the PDPC to consider amending the PDPA to include specific baseline provisions addressing biometric data. Such provisions should prescribe a higher standard in the manner that an organisation collects, uses, retains and stores biometric data.

Grounds of Decision

## Re Singapore Telecommunications Limited and another

## [2018] PDP Digest 148

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-1603-A652
**Decision Citation**: [2018] PDP Digest 148; [2017] SGPDPC 4

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

6 April 2017

### BACKGROUND

1 This is a case where an error made by Tech Mahindra (Singapore) Pte Ltd ("Tech Mahindra") in updating a database resulted in the personal particulars of a single customer ("Affected Customer") replacing personal particulars in the profiles of numerous users of Singapore Telecommunications Limited ("Singtel"). Consequently, the Affected Customer's personal particulars could be viewed by the other Singtel customers on the MySingtel mobile application ("MySingtel Application") and the MyBill (<mybill.singtel.com>) and MyAccount (<myaccount. singtel.com>) portals on Singtel's website.

2 The main issue in the investigation was whether the organisations breached their protection obligation under s 24 of the Personal Data Protection Act 2012[1] ("PDPA"). The following sets out the Personal Data Protection Commission's ("Commission") findings on the matter.

1 Act 26 of 2012.

## MATERIAL FACTS AND DOCUMENTS

3 Singtel is a telecommunications company that had, as part of its services, a single sign-on service for its customers, allowing them to use the same access credentials to access his or her different Singtel accounts and bills across Singtel's applications and portals. This service is known as ONEPASS. Singtel had engaged Tech Mahindra, an information technology ("IT") vendor, to provide application development, maintenance and support services for ONEPASS ("ADMS Services"). This includes updating customer profiles in the ONEPASS database.

4 The genesis of this matter can be traced to when Singtel and Tech Mahindra had sought to rectify an issue with the Affected Customer's ONEPASS account. On 26 February 2016, the Affected Customer had informed Singtel about the login difficulties with his ONEPASS account. Following this, Singtel escalated the Affected Customer's issue to Tech Mahindra. Tech Mahindra subsequently determined that an update was needed to the Affected Customer's profile on the ONEPASS database, and executed a database script to update the profile.

5 On 29 February 2016, Singtel received several reports from ONEPASS users. These affected different systems in different ways. Some customers reported that their MySingtel Application profile had been modified to reflect the Affected Customer's account number, billing address and services. A number of Singtel customers also reported that the NRIC field in their ONEPASS profiles on the MyBill and MyAccount portals had been modified to reflect the Affected Customer's NRIC number. Apart from these, all other personal details of the user, such as the user's name and address, remained unaffected.

6 A total of 2.78 million ONEPASS users' accounts were affected, out of which 2,518 users had viewed the Affected Customer's NRIC number through the MySingtel Application before Singtel disabled access to the MySingtel Application.

7 Shortly after receiving reports of the incident, Singtel shut down the MySingtel Application and disabled access to the ONEPASS profile webpages on the MyBill and MyAccount portals. Singtel also notified the Affected Customer of the incident.

8 Singtel's investigations disclosed that the incident was caused by a coding issue in the database script that was executed by Tech Mahindra.

The Tech Mahindra employee who prepared the database script had omitted a "where" clause in the script, which was required to limit the application of the changes to the Affected Customer's profile. This was in breach of standard operating procedures that were in place at that time.

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

### *Issues for determination*

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

(a) whether Tech Mahindra was acting as a data intermediary for Singtel in relation to the ONEPASS users' personal data; and

(b) whether each of the organisations complied with its obligation under s 24 of the PDPA in respect of the data breach incident.

### *Issue (a): Whether Tech Mahindra was acting as a data intermediary for Singtel in relation to the ONEPASS users' personal data?*

10 Tech Mahindra was engaged by Singtel to provide ADMS Services, which covered a range of support activities such as troubleshooting, incident management and application maintenance services, including ONEPASS and single sign on services. Crucially, Tech Mahindra was also granted access to Singtel's database to maintain customer profiles on the ONEPASS database. The maintenance of customer profiles amounts to "processing" personal data on behalf of Singtel. Accordingly, it was acting as a data intermediary (as defined in s 2(1) of the PDPA) of Singtel.

11 A data intermediary has a duty to comply with the protection obligation under s 4(2) of the PDPA. At the same time, the organisation has the same obligation in respect of personal data processed by a data intermediary on its behalf and for its purposes as if the personal data were processed by the organisation itself under s 4(3) of the PDPA.

12 In accordance with ss 4(2) and 4(3) of the PDPA, both Singtel and Tech Mahindra have concurrent obligations to make reasonable security arrangements to protect the personal data of Singtel customers that are in their possession and/or under their control.

***Issue (b): Whether each of the organisations complied with its obligation under section 24 of the Personal Data Protection Act in respect of the data breach incident?***

*Singtel*

13 In this case, the Commission finds Singtel to have complied with its obligation under s 24 of the PDPA to put in place reasonable security arrangements to protect personal data.

14 First, Singtel had put in place a contract requiring Tech Mahindra to comply with the PDPA, adhere to all of Singtel's access and security policies, processes and directions, and to ensure that its employees are trained to comply with all data protection laws and security measures before it is given control and access to the personal data in Singtel's systems. Having a contract that sets down the obligations and responsibilities of a data intermediary to protect personal data is a prudent first step for organisations to take. One of the key benefits of having such a contract is that it would make clear the parties' respective roles, obligations and responsibilities to protect the personal data.

15 Second, Singtel had also followed through with operational procedures and checks to ensure that Tech Mahindra carried out its functions to protect personal data. Singtel and Tech Mahindra had a standard operating procedure ("SOP") governing the management of the ONEPASS database. If a database script change was required, the employee making the change was required to run the database script in the development environment before running the database script in the actual production environment. In this way, any errors or issues arising from the database script are contained in the test-bedding environment without impacting on or affecting the live system. This enables an organisation to detect and rectify any issues or errors in the script before the actual implementation.

16 Singtel had also given Tech Mahindra specific instructions for the updating of the Affected Customer's profile on the ONEPASS database. In an e-mail on 2 April 2015, Singtel made specific reference to the "where" clause in the database script and gave specific instructions that the "where" clause of each database update script had to be a primary key, *ie*, it could not be left blank. The function of the "where" clause is to introduce a restrictive parameter on the operation of the programmatic instructions to

specific records, columns or tables in the database. In this case, by specifying the Affected Customer's record in the "where" clause, the database script would have selected only his record for the operation.

17 Third, Singtel conducted annual on-site security reviews of Tech Mahindra's off-site premises as part of its governance process and required Tech Mahindra to confirm its compliance with various security protocols. Singtel also conducted penetration tests on the MySingtel Application, the MyAccount and MyBill portals as well as the ONEPASS system and fixed the vulnerabilities, which were unrelated to the data breach incident, found during the penetration tests.

18 In light of the above, the Commission finds that Singtel made reasonable security arrangements in compliance with the protection obligation under s 24 of the PDPA.

*Tech Mahindra*

19 The Commission, however, finds Tech Mahindra to be in breach of its obligation, as a data intermediary, under s 24 of the PDPA.

20 The Commission finds that even though there were in place internal SOPs and policies regarding the modification or processing of personal data in the ONEPASS database by Tech Mahindra, it failed to comply with them during the actual handling and management of the personal data.

21 First, notwithstanding Singtel's e-mail instructions to include the "where" clause in the database script, Tech Mahindra failed to comply with the instructions, and left it out from the database script.

22 Second, Tech Mahindra did not comply with Singtel's SOP highlighted at [15] above. Tech Mahindra did not check that the database script was functioning properly in a test-bedding environment before execution in the production environment. Consequently, the personal data of 2.78 million ONEPASS users were modified and replaced by personal data from the Affected Customer when Tech Mahindra executed the database script containing the erroneous code.

23 Third, although Tech Mahindra implemented internal security arrangements, it did not adhere to its own SOPs. Tech Mahindra had a practice (which was not documented) for the database update script to be reviewed by a more senior member of the support team before execution.

Additionally, employees were also expected to verify that an update was correct after the execution of the database update script. However, in this case, both these layers of checks were omitted.

24 In the Commission's assessment, given the above failures and missteps, Tech Mahindra failed to make reasonable security arrangements to protect the personal data of Singtel customers that it processed on behalf of Singtel. Accordingly, Tech Mahindra is in breach of s 24 of the PDPA.

## PERSONAL DATA PROTECTION COMMISSION'S DIRECTIONS

25 In exercise of the power conferred upon the Commission pursuant to s 29 of the PDPA, the Commission directs that Tech Mahindra pay a financial penalty of $10,000 within 30 days from the date of the Commission's direction.

26 In assessing the breach and remedial directions to be imposed, the Commission considered various factors relating to the case, including the mitigating and aggravating factors set out below:

(a) the personal data disclosed in the data breach incident, particularly the Affected Customer's NRIC number, are of a sensitive nature;

(b) not only was the Affected Customer's NRIC number disclosed without authorisation, there was also an unauthorised modification of the personal data of 2.78 million ONEPASS users;

(c) the data breach incident could have been avoided if Tech Mahindra had followed Singtel and Tech Mahindra's SOPs;

(d) of the 2.78 million ONEPASS users whose accounts had been modified, only 2,518 users had viewed the Affected Customer's NRIC number;

(e) Tech Mahindra and Singtel had jointly notified the Commission of the data breach incident, and were co-operative in the course of the investigation; and

(f) Singtel and Tech Mahindra took prompt remedial and preventative actions.

27 The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA. Organisations should take the necessary action to ensure that they comply with their obligations under

the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisations accordingly.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re National University of Singapore

## [2018] PDP Digest 155

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1605-B0028
**Decision Citation**: [2018] PDP Digest 155; [2017] SGPDPC 5

***"Personal data"*** *– Student matriculation number*
***Protection Obligation*** *– Disclosure of personal data – Insufficient administrative security arrangements*
***Protection Obligation*** *– Staff training*

26 April 2017

### BACKGROUND

1 A student of the organisation ("Organisation") had complained to the Personal Data Protection Commission ("Commission") that a URL link that was being circulated for the Organisation's orientation camp had disclosed (without authorisation) the personal data of student volunteers from the College of Alice and Peter Tan ("CAPT"). CAPT is a residential college of the Organisation.

2 It was found that by following the URL link, one could access an online Excel spreadsheet containing the full names, mobile numbers, matriculation numbers, shirt sizes, dietary preferences, dates of birth, dormitory room numbers and e-mail addresses ("personal data set") of approximately 143 student volunteers. The student matriculation number is a unique student identification number issued by the Organisation. The matriculation number to a student is, in a limited sense, like an NRIC number to a Singapore citizen and permanent resident, in that it is required for various school activities, such as accessing online library resources, or for the submission of examination scripts.

3 Based on the complaint that was made, the Commission proceeded to investigate into an alleged breach by the Organisation of the protection

obligation under s 24 of the Personal Data Protection Act 2012[1] ("PDPA"). The following sets out the Commission's findings following its investigations into the matter.

## MATERIAL FACTS AND DOCUMENTS

4 The CAPT Freshman Orientation Camp ("FOC") is an annual event organised by student volunteers from CAPT for the freshmen matriculating into the Organisation. The FOC in the present case was for the year 2016.

5 The Organisation had designated several student leaders to take the responsibility for organising the FOC. As part of the process of organising the FOC, these student leaders would recruit other student volunteers to participate as counsellors and assist in the running of the FOC.

6 To get themselves organised, the student leaders created an online form using Google Forms[2] for the student volunteers to fill in their personal particulars. The particulars that were entered into the Google Forms were stored in a Google Sheets[3] spreadsheet ("Spreadsheet"), which compiled all the particulars of the various student volunteers in a single spreadsheet.

7 The Spreadsheet was meant to be shared amongst the student leaders only, and not to the student volunteers, or anyone else. For the purpose of sharing access to the Spreadsheet, a URL link to the Spreadsheet was generated through Google Sheets by selecting the "Share with specific people" function, and this URL link was then shared amongst the student leaders. Only specified persons could access the Spreadsheet as the URL link to the Spreadsheet required a user to first log in with his or her Google account.

8 While the Spreadsheet was initially circulated to specified people (*ie*, the student leaders), at some point in May 2016, the Spreadsheet came

---

1 Act 26 of 2012.

2 An online form creation application by Google. Users can create, edit and distribute the form easily, and save responses into a Google Sheet. See <https://www.google.com/forms/about/> for more information.

3 An online spreadsheet application by Google, which enables users to create, edit and share spreadsheets. Sharing spreadsheets allows multiple users to edit the same spreadsheet at the same time. See <https://www.google.com/sheets/about/> for more information.

to be circulated beyond the originally intended group. An unknown party, whether intentionally or otherwise, changed the setting on the Spreadsheet from "Share with specific people" to "Share using a link". As a result, any user who possessed the URL link could access the Spreadsheet, and all the personal data set of the student volunteers contained within.

9 Consequently, the personal data set was now exposed to those who had access to the URL link, which may have extended to persons beyond the Organisation itself.

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

10 The Organisation has not shied away from its responsibility for the data breach incident, and has confirmed that the FOC was an event that it had sanctioned. The Organisation has mentioned that any act done in the name of CAPT, which was authorised by the Organisation, was an act done in the name of the Organisation.

11 Given that the FOC activities were carried out in the Organisation's name, the Organisation is ultimately responsible for ensuring that the personal data of its students are adequately protected pursuant to s 24 of the PDPA.

12 In light of the events of this case, the relevant issue for determination is whether the Organisation had indeed complied with s 24 of the PDPA.

### *Whether the Organisation was in breach of section 24*

13 In its response to the Commission during investigations, the Organisation did not dispute the fact that the data breach had occurred. However, the fact that the data breach occurred is not necessarily indicative of a contravention of the PDPA. Rather, it is necessary to consider whether the Organisation's safeguards that were in place at the material time were adequate having regard to the volume and type of personal data in question, and whether the safeguards were reasonable in the circumstances.

*The Organisation's security arrangements at material time*

14 Security arrangements to protect personal data may take various forms, including administrative, physical, technical measures or a combination of these. According to the Organisation, it had, at the material time, implemented administrative safeguards, in the form of data protection training and guidelines, to adequately protect the personal data set in its possession and under its control:

> (a) Data protection training: The Organisation conducted classroom training in or around 2014 on the relevant data protection obligations that apply to the collection, use and disclosure of personal data for selected students who were likely to hold leadership roles. However, it would appear that the classroom training did not carry over to 2015. In 2015, the Organisation had instead provided all its students with access to e-training on the PDPA. This e-training appeared on the list of trainings available on the Integrated Virtual Learning Environment ("IVLE") portal such that when students logged into the system, the e-training option would be visible to them.
> (b) Data protection guidelines: The Organisation issued guidelines for the students organising various events in the name of the Organisation to ensure that all student activities complied with the Organisation's regulations. These guidelines were adapted to become the *CAPT Event Planning Guidelines for Student Groups* ("CAPT Guidelines"). The CAPT Guidelines contained a section titled "Responsible Usage and Access of Personal Data". Students in charge of planning activities in the name of the Organisation who collected personal data, such as "name, Matric No., email address, HP number", were reminded to "observe proper use and access to prevent potential data leakage and unauthorized/accidental access".

*The Organisation did not provide adequate training for student leaders*

15 Although the Organisation had in place general policies and guidelines for the protection of personal data, when it came to the security arrangements on the ground, the Organisation did not have any formalised data protection training in place to train and equip its students with the mind-set, knowledge, skills and tools to protect personal data.

16 While the Organisation had made the e-training programme available on IVLE, the Organisation did not make it compulsory for all the student

leaders of the FOC to undergo the e-training. In any case, the Organisation confirmed that none of the student leaders had undergone the e-training prior to the commencement of the FOC in 2016, even though the student leaders were involved in the handling of the personal data of other students.

17 With regard to classroom training, it appeared to have been held only once in 2014, and was only for the benefit of selected students. Although the Organisation claimed that it had plans to make this classroom training an annual event, no such plans had materialised by the time of the FOC in 2016.

18 In this regard, there was effectively no data protection training provided to the student leaders of the FOC in 2016.

19 By the Organisation's failure to provide adequate training for the student leaders before they handled personal data, this increased the risk of a data breach occurrence. Even if a student leader had some knowledge of the PDPA, how that translated into the actual practice of protecting personal data was something that the Organisation would not be able to ensure.

20 We pause to set out how training falls as a consideration for ensuring adequate protection of personal data under the PDPA.

*Training as a type of security arrangement*

21 Data protection training may fall under two separate data protection obligations – the openness obligation (ss 11 and 12 of the PDPA) and the protection obligation (s 24 of the PDPA). An organisation that is subject to the openness obligation is required to communicate to its staff information about its policies and practices, pursuant to s 12(*c*) of the PDPA. This communication of the data protection policies may necessarily involve some form of staff training.

22 While the openness obligation may not extend to student leaders who are not members of staff, data protection training may also be seen as an administrative security measure that is necessary for compliance with the protection obligation. In its advisory guidelines, the Commission provided examples of administrative security measures such as the conducting of "*regular training sessions for staff* to impart good practices in handling

personal data and strengthen awareness of threats to security of personal data"[4] [emphasis added].

23 In the UK, administrative or organisational security measures may encompass relevant and appropriate training of staff on the data protection obligations of the organisation, especially for employees that collect, use or disclose personal data.[5] In describing the management and organisational measures that an organisation should put in place, the UK's Information Commissioner's Office highlighted the importance of staff training and stated that:[6]

> It is vital that your staff understand the importance of protecting personal data; that they are familiar with your organisation's security policy; and that they put its security procedures into practice. So you must provide *appropriate initial and refresher training* …. [emphasis added]

24 Similarly, in Canada, the Office of the Information and Privacy Commissioner for British Columbia expressly stated in the case of *Park Royal Medical Clinic* that "administrative security, which encompass policies and training regarding privacy is another important component" of the obligation to make reasonable security arrangements.[7] 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:[8]

> … [d]iligent and consistent execution of security policies and procedures [which] depends to a large extent on ongoing privacy training of staff and

---

4 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at para 17.5.

5 Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (Oxford University Press, 4th Ed, 2015) at p 126.

6 Information Commissioner's Office, *Information security (Principle 7)* (25 October 2016) <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/> at p 4.

7 *Order P15-01: Park Royal Medical Clinic* 2015 BCIPC 20 <https://www.oipc.bc.ca/orders/1783> at para 58.

8 *PIPEDA Case Summary #2008-395: Commissioner initiates safeguards complaint against CIBC* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2008/pipeda-2008-395/>, second bullet point in the "Lessons Learned" section at p 1.

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".[9]

26 In Hong Kong, the Office of the Privacy Commissioner for Personal Data stated in its Code of Practice on Human Resource Management that employees "play the principal role in implementing an employer's policies on the security of personal data". Organisations should take reasonably practicable measures to ensure that employees handling personal data are trained to observe the personal data privacy policies, exercise due diligence in the application of those policies, and are subject to procedures designed to ensure their compliance with those policies.[10] This statement is in line with Principle 4 of Hong Kong's Personal Data (Privacy) Ordinance, *ie*, security of personal data.[11]

27 Overall, the foreign data protection authorities all seem to agree that the data protection training provided by an organisation may constitute a type of administrative or organisation security measure, and that this training has an impact on the proper implementation of that organisation's data protection policies and practices.

28 The above positions are useful in our case here. In the Commission's view, a formalised data protection training for the student leaders for the FOC would be beneficial in several aspects. Not only would it inform the student leaders of the PDPA, but it would also sensitise them to their personal data protection obligations. Further, it also trains the students on

---

9 *PIPEDA Report of Findings #2016-005: Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/ Acting Australian Information Commissioner* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/> at [74].

10 Office of the Privacy Commissioner for Personal Data, Hong Kong, *Code of Practice on Human Resource Management* (April 2016) (First Revision) <https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf> at para 1.4.1.

11 Personal Data (Privacy) Ordinance (Cap 486) (Hong Kong) Schedule 1, Principle 4.

the practices to be adopted, and not just pay lip service to the PDPA obligations, or to the Organisation's policies. Additionally, it may provide some guidance for students to go about their tasks when it comes to handling personal data.

*The Organisation's breach of section 24 of the Personal Data Protection Act*

29 As mentioned above, the Organisation did not have in place any formalised training for the student leaders, even though it was reasonably foreseeable that they would be handling personal data in the course of organising the FOC.

30 The FOC was an event that involved many students, and would potentially involve the handling of many students' personal data. The Organisation ought to have at least ensured that the student leaders organising and running the FOC had the proper training to deal with and protect the personal data that they would handle. Moreover, since the FOC was an event that took place annually, the Organisation could have anticipated and planned for some form of training to be provided to the student leaders who were handling the personal data.

31 Since the FOC is an annual event, the training that can be provided can also be customised to the FOC and the data processing activities that will foreseeably be carried out. Such customisation could be based on considerations such as (a) to whom the training should apply (*ie*, confined to just the student leaders or extending also to student volunteers); (b) the most effective way of disseminating best practices to all who may come into contact with personal data; and (c) the frequency and timing of such training. To be clear, the Commission is not setting down any rule that mandates formalised classroom training. The Organisation should adopt a mode of training that it considers to be effective and expedient, having regard to these factors.

32 In this case, it was not enough for the Organisation to rely solely on the CAPT Guidelines in order to protect personal data. Apart from the fact that it was unclear whether the student leaders were fully apprised of the CAPT Guidelines, the CAPT Guidelines did not necessarily translate into actual processes that would enable the student leaders to comply with the data protection obligations in practice. Proper guidance is not easily

substitutable or replaceable by general guidelines that an organisation may set.

33 In view of the fact that the Organisation did not put in place adequate training for the student leaders, the Commission finds that the Organisation failed to make reasonable security arrangements to protect the personal data in its possession and/or under its control and is in breach of s 24 of the PDPA.

## PERSONAL DATA PROTECTION COMMISSION'S DIRECTIONS

34 The Commission 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 $1m as the Commission thinks fit.

35 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commission took into account the following factors:

(a) a significant number of individuals (approximately 143 students) were affected by the data breach incident;

(b) the potential adverse consequences from a misuse of the student matriculation number by other persons. For example, passing off as a student to carry out identity theft, or even carrying out pranks or nuisances in the student's name. It was, however, noted that the student matriculation number is used as an identifier for the duration of the student's undergraduate or postgraduate course and not for an extended period of time; and

(c) the Organisation was co-operative with the Commission and forthcoming in its responses during the Commission's investigation.

36 Pursuant to s 29(2) of the PDPA, and having completed its investigation and assessment of this matter, the Commission is satisfied that the Organisation was in breach of the protection obligation under s 24 of the PDPA. The Commission has decided to issue directions to the Organisation, pursuant to s 29 of the PDPA, in respect of the Organisation's breach of s 24 of the PDPA.

37 The Commission had provided its preliminary grounds of decision and directions to the Organisation directing the Organisation to essentially (a) implement mandatory training for its student volunteers within 60 days and (b) provide an update to the Commission of the training arrangements it had put in place.

38 The Organisation's Data Protection Office accepted the Commission's findings but made representations in respect of the preliminary directions, requesting:

> (a) for a longer duration of 120 days for the Organisation to fully implement the necessary training modules for its student leaders, which will apply to not just future freshman activities, but for other activities sanctioned by the Organisation; and
> (b) that the direction for mandatory training should refer to "student leaders", which should take the following suggested meaning: "any undergraduate or post graduate student of [NUS] who has been appointed or is part of any committee tasked to organize any event/activity officially approved or sanctioned by [NUS]".

39 The Commission has considered and accedes to the representations. While the Commission generally has the power to impose such directions as it deems fit in the circumstances, the Commission is prepared to consider representations from organisations on the grounds of decision and the form of directions to be issued, especially since directions ought to be adapted or customised to their operations or practices to be *effective* in addressing the particular shortcomings that had been identified during investigations. In the present case, the Commission accepts the representations since they do not detract from the key principles, functions and purposes of the Commission's grounds of decision and directions.

40 However, the Commission clarifies that its directions are tailored to enable the Organisation to effectively address the shortcomings that had been identified during investigations. In this regard, while the Organisation has been directed to put in place mandatory training for student leaders of officially approved or sanctioned activities, that does not mean that for other types of activities, there is no need for the Organisation to put in place policies, create awareness or provide voluntary training. The PDPA imposes a free standing and continuing obligation on the Organisation to ensure that its policies are effective in implementing the requisite standard of personal data protection. It behoves the Organisation to consider

whether, beyond the directions issued in this case, any further arrangements are necessary.

41 Having carefully considered all the relevant factors of this case, the Commission hereby directs:

(a) the Organisation to, within 120 days from the date of the Commission's directions:

(i) design training (including online training and dissemination of training materials) that would address personal data protection in the context of the collection and processing of personal data for student events and of the resulting interaction;

(ii) make arrangements for such training to be mandatory for any student leader. For the avoidance of doubt, a student leader is defined as any undergraduate or postgraduate student of the Organisation who has been appointed or is part of any committee tasked to organise any event or activity officially approved or sanctioned by the Organisation;

(iii) make other arrangements as would be reasonably required to meet the objectives in [41(a)(i)] and [41(a)(ii)] above; and

(b) by no later than 14 days after the above action has been carried out, the Organisation shall, in addition, submit to the Commission a written update providing details on the arrangements for the training for student leaders managing personal data for student events officially approved or sanctioned by the Organisation.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

## Re Tiger Airways Singapore Pte Ltd and others

## [2018] PDP Digest 166

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1607-B0129
**Decision Citation**: [2018] PDP Digest 166; [2017] SGPDPC 6

***Data intermediary*** *– "Processing" of personal data*
***Protection Obligation*** *– Access to personal data – Insufficient technical, physical and administrative security arrangements*

31 May 2017

### INTRODUCTION

1 On 27 July 2016, the Personal Data Protection Commission ("Commission") received a complaint that the passenger name list for Tiger Airways Singapore Pte Ltd ("Tigerair") flight TR2466 ("Flight Manifest") had been improperly disposed of in a rubbish bin in the gate hold room at Changi Airport. The complainant alleged that the Flight Manifest could have been retrieved by anyone in the vicinity.

2 The Commission undertook an investigation into the matter and sets out its findings and grounds of decision below.

### MATERIAL FACTS

3 Tigerair is a low-cost carrier. SATS Ltd ("SATS") is an aviation ground handling service provider. SATS was engaged by Tigerair to provide ground handling services. In accordance with the terms of the ground handling services contract between SATS and Tigerair ("Ground Handling Services Contract"), SATS was responsible for the provision of the services by its subsidiaries as if it had been provided by SATS itself.

4 Asia-Pacific Star Private Limited ("APS") is a wholly-owned subsidiary of SATS. SATS subcontracted the provision of ground handling services for

Tigerair to APS pursuant to a Services Agreement dated 11 June 2014 ("Services Agreement").

5 Under the Services Agreement, APS was responsible for managing the boarding process, reconciling passenger numbers and verifying travel documents at the boarding gate. Among other things, APS was required to print a copy of the Flight Manifest at the boarding gate for the cabin crew to take on board the flight and submit to the immigration authority at the arrival destination.

6 On 26 July 2016, an APS employee who was on gate duty for flight TR2466 ran out of paper while printing a copy of the Flight Manifest. The APS employee disposed of the partially-printed Flight Manifest in the rubbish bin in the gate hold room for flight TR2466 and reprinted the Flight Manifest in full ("Data Breach Incident"). The gate hold room where the partially-printed Flight Manifest was discarded was only accessible to passengers and airport staff.

7 None of the organisations ("Organisations") (nor the complainant) could verify the exact number of passengers whose personal data were disclosed in the partially-printed Flight Manifest.

8 The partially-printed Flight Manifest contained passenger personal data such as the passenger's name, booking reference number (also known as PNR), fare class, sequence number of check-in, date of booking, seat number, destination and flight number.

9 Other personal data such as the passenger's full name, passport number, home address, phone number, e-mail address and last four digits of the credit card used to pay for the plane ticket could have been retrieved by entering the passenger's name and the PNR into Tigerair's "Manage My Booking" portal. Special features or add-ons to the passenger's flight(s) and travels, such as hotel bookings and airport transfers or cars rentals, would also have been reflected on the "Manage My Booking" portal. This information was only accessible up to the last travelling date of the passenger's itinerary.

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

10 At the outset, the Commission finds that the partially-printed Flight Manifest constitutes personal data as defined in s 2(1) of the Personal Data

Protection Act 2012[1] ("PDPA"). The Flight Manifest contained data about the passengers who could be identified either from that data alone or from that data and the data on Tigerair's "Manage My Booking" portal.

### *Issues for determination*

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

(a) whether SATS and APS were acting as data intermediaries for Tigerair in relation to the Tigerair passengers' personal data; and

(b) whether each of the Organisations complied with its obligation under s 24 of the PDPA in respect of the Data Breach Incident.

### *Issue (a): Whether SATS and APS were acting as data intermediaries for Tigerair in relation to the Tigerair passengers' personal data*

12 As mentioned at [3] above, SATS was engaged by Tigerair to provide services such as managing the boarding process, reconciliation of passenger numbers and verification of travel documents at the boarding gate. These are activities of "processing" personal data on behalf of Tigerair as defined in s 2(1) of the PDPA.

13 SATS had subcontracted the provision of the services to APS but remained responsible for the provision of ground handling services as if they were performed by SATS itself. APS was granted access to Tigerair's "Departure Control System" which contained all the information related to a passenger's booking to carry out activities of "processing" on behalf of Tigerair. Accordingly, the Commission is satisfied that SATS and APS were both acting as data intermediaries of Tigerair.

14 A data intermediary has a duty to comply with the protection obligation under s 4(2) of the PDPA. An organisation has the same obligation in respect of personal data processed by a data intermediary on its behalf and for its purposes as if the personal data were processed by the organisation itself under s 4(3) of the PDPA. Accordingly, Tigerair, SATS and APS each have an obligation to make reasonable security arrangements to protect the personal data of Tigerair passengers in their possession and/or under their control.

---

1 Act 26 of 2012.

***Issue (b): Whether each of the Organisations complied with its obligation under section 24 of the Personal Data Protection Act in respect of the Data Breach Incident***

15 It was not disputed that the partially-printed Flight Manifest was improperly disposed of by the APS employee at the gate hold room. However, the Organisations represented that they had adequate policies and processes regarding the protection of personal data. The Data Breach Incident was simply an isolated incident that occurred due to the oversight of the APS employee.

16 Section 24 of the PDPA places a positive obligation on an organisation to make reasonable security arrangements to protect the personal data in its possession or under its control and to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

17 In accordance with s 11(1) of the PDPA, the reasonableness of security arrangements made is objectively determined, having regard to what a reasonable person would consider appropriate in the circumstances. 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.

18 In assessing the reasonableness of security arrangements, the Commission will also take into consideration the factors set out in the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*:

(a) the nature of the personal data;

(b) the form in which the personal data have been collected (*eg*, physical or electronic); and

(c) the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

*Tigerair*

19 As an organisation under the PDPA, Tigerair has the primary responsibility of ensuring that there are reasonable security arrangements in place to protect the personal data in its possession or under its control.

Tigerair remains ultimately responsible even though it had engaged a data intermediary to provide ground handling services and process personal data on its behalf.

20 Under the Ground Handling Services Contract, Tigerair required SATS to establish and maintain local procedures to comply with the PDPA in its provision of services to Tigerair.

21 SATS was also required to carry out all services in accordance with Tigerair's ground services manual ("Ground Services Manual"). The Ground Services Manual specifically provided that ground handlers were to adhere to the requirements of the PDPA, including the obligations to use personal data only for the purposes for which consent had been obtained, protect personal data in its custody, and prevent disclosure to unauthorised persons.

22 In the present context, the ground handling services fell under the responsibility of SATS and APS, both of whom had the responsibility of ensuring that in the provision of these services, personal data were adequately protected. In this regard, having imposed a contractual obligation on SATS to establish and maintain local procedures to comply with the PDPA, the Commission finds it reasonable for Tigerair to have expected SATS to carry out its obligations in accordance with the contract and the relevant sections of the Ground Services Manual.

23 Further, given that SATS was contractually accountable for APS's provision of services, it was reasonable for Tigerair to have expected SATS to ensure that APS would implement reasonable security arrangements to protect the personal data that it processed on behalf of Tigerair. This is especially since Tigerair did not have oversight over the actions of APS's employees.

24 Accordingly, the Commission finds that Tigerair had complied with its protection obligation under s 24 of the PDPA.

*SATS*

25 SATS had, in its Services Agreement with APS for the subcontracting of ground handling services for Tigerair, expressly required APS to comply with and ensure that the ground handling services were provided and performed in a manner which did not infringe any applicable laws, regulations and directions, including the PDPA.

26 In addition, SATS implemented the SATS Group Code of Conduct ("Group Code of Conduct"), which required all employees who may handle, receive, collect, use, disclose or transfer any personal data to comply with the PDPA and the Personal Data Protection Policy ("Group Data Protection Policy").

27 The Group Data Protection Policy sets out guidelines on the physical measures that should be undertaken to protect personal data. Specifically, the guidelines recommended that there should be proper and secure disposal of documents containing personal data, such as requiring such documents to be shredded. APS was required to comply with both the Group Code of Conduct and the Group Data Protection Policy as it was a member of the SATS Group.

28 SATS also sent periodic updates and reminders to the SATS Group management and staff (including those from APS) to remind them about their data protection obligations under the Group Code of Conduct and the Group Data Protection Policy. Pertinently, SATS conducted annual "Control Self-Assessment" exercises as part of its enterprise risk management and required the General Manager of APS to confirm APS's compliance with the Group Data Protection Policy.

29 In view of the above, the Commission finds that SATS made reasonable security arrangements and fulfilled its protection obligation under s 24 of the PDPA.

*APS*

30 APS represented that it had put in place security arrangements and the Data Breach Incident was an isolated incident that occurred as a result of a lapse by an APS employee. Pursuant to s 53(1) of the PDPA, any act done or conduct engaged in by an employee in the course of his employment shall be treated 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. Accordingly, APS remains responsible for its employee's conduct.

31 Although the Commission finds that APS did have some security arrangements in place, the Commission is not satisfied that APS fulfilled its protection obligation under s 24 of the PDPA.

32 As mentioned at [27] above, APS is part of the SATS Group, all APS employees are required to comply with the Group Code of Conduct and the Group Data Protection Policy. The Group Code of Conduct was annexed to APS employees' letters of employment and all new APS employees received a briefing on the requirement to comply with the PDPA during their employee induction programme.

33 However, APS relied solely on the administrative safeguards implemented by SATS, which applied to the organisations within the SATS Group. There was no evidence that APS provided additional information or implemented additional safeguards in order to contextualise the group level policies to its ground operations. In line with the Commission's observation in *Re National University of Singapore*[2] that general guidelines did not necessarily translate into the kind of practices that were actually needed on the ground to protect personal data, it is likewise important here for organisations to ensure that an organisation's policies and training have to be contextualised to its operational setting. In this case, there was no evidence that APS had any procedure or policy of its own apart from the SATS Group Data Protection Policy.

34 Crucially, given that the personal data found in the Flight Manifest provided further access to personal information of an even more sensitive nature found on the "Manage My Bookings" portal, the impact to the passengers from the improper disposal was higher. Given the potential adverse consequences of unauthorised access to that personal data (from the initial and secondary exposure), APS should have afforded a high level of protection to such personal data, with greater attention given to the proper disposal of documents containing such personal data. The specific scenarios (like the present) where there are risks of data leaks through inappropriate handling or disposal of Flight Manifests that are likely to arise in ground operations (*eg*, staff handling Flight Manifests at the gates) ought to have been part of the effort to translate and contextualise the group level policies for APS's specific circumstances.

35 Additionally, as the Commission observed in *Re National University of Singapore*,[3] security policies and procedures are essential but they are only effective when properly and consistently implemented and followed by

2 [2018] PDP Digest 155 at [32].

3 [2018] PDP Digest 155 at [25].

employees. Ongoing training on the organisation's data protection obligations and the organisation's data protection policies and procedures is key to fostering and maintaining a high organisational awareness of data protection concerns and to ensure that the data protection obligations under the PDPA are consistently understood and acted upon by employees. This was also observed by the Commission in *Re National University of Singapore*.[4] Yet, as set out at [32] above, the only training that APS employees appeared to have received was a general data protection briefing during the employee induction programme for new employees.

36 APS should have provided customised training and regular refresher training for APS employees who routinely handled passengers' personal data. APS processes the personal data of a large number of individuals, including passenger identification information such as the Flight Manifest, on a regular basis in the course of its duties.

37 Given the Commission's findings on the lack of administrative and physical safeguards in place, the Commission finds that APS did not make reasonable security arrangements to protect the personal data it processed on behalf of Tigerair.

## PERSONAL DATA PROTECTION COMMISSION'S DIRECTIONS

38 For the reasons set out above, the Commission has determined that APS did not comply with its protection obligation under s 24 of the PDPA. In exercise of the power conferred upon the Commission pursuant to s 29(1) of the PDPA, the Commission directs APS to:

(a) conduct a review of its procedure for proper disposal of personal data in its possession and/or control;

(b) introduce data protection policies that are contextualised and pertinent to the services provided by APS and functions performed by its staff; and

(c) include a programme for initial and refresher training on its implementation by the APS staff in the course of its operations.

39 In assessing the breach and remedial directions to be imposed (including not imposing a financial penalty on APS in this case), the

4 [2018] PDP Digest 155 at [20]–[28].

Commission considered various factors relating to the case, including the mitigating factors set out below:

(a) the gate hold room where the Flight Manifest was disposed of was accessible only by passengers and airport staff;

(b) the bin where the Flight Manifest was disposed of could reasonably be expected to be emptied regularly as part of routine maintenance;

(c) the Flight Manifest held data that served as login credentials to individual passengers' personal data on the "Manage My Bookings" portal. However, the information on the page was only accessible for a limited time until the last travelling date on the passenger's itinerary; and

(d) there were no complaints of any actual unauthorised access to the "Manage My Bookings" page of any passenger.

40 The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA. Organisations should take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisations accordingly.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

**Re Furnituremart.sg**

**[2018] PDP Digest 175**

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1611-B0319
**Decision Citation**: [2018] PDP Digest 175; [2017] SGPDPC 7

***Protection Obligation*** *– Disclosure of personal data – Insufficient administrative security arrangement*

31 May 2017

## BACKGROUND

1 This is a case involving an organisation ("Organisation") which had issued to its customer ("Complainant") an invoice which had a separate invoice ("second invoice") containing personal data of another customer printed on the reverse side. In this regard, the other customer's personal data were disclosed to the Complainant, comprising of the following information of the other customer:

(a) customer's surname;
(b) home address;
(c) delivery address;
(d) telephone number; and
(e) e-mail address.

2 The Complainant made a complaint to the Personal Data Protection Commission ("Commission") on 7 November 2016 of the disclosure that was made, and the Commission conducted an investigation into the matter. It now sets out its findings of its investigations below.

## MATERIAL FACTS AND DOCUMENTS

3 The Organisation is in the business of trading furniture, bedding and other domestic products.

4 Whenever it issues its invoices, the Organisation's procedure is to make three copies of every invoice: the first for the Organisation's filing, the second for the customer, and the third for the customer to sign and return to the Organisation on delivery of the goods.

5 According to the Organisation, all signed copies of invoices are supposed to be returned to its office, and subsequently destroyed by its staff on a daily basis.

6 In this case, however, the returned invoice was put in a printer feed tray, and reused as printing paper for the complainant's invoice.

7 In support of the foregoing, the Organisation provided the Commission with a document entitled, "Policies and internal guideline [*sic*] for the protection of personal data of customers as at November 2016". The document provided for, amongst other things: (a) all invoices to be printed on new paper; (b) the supervisor to check that the invoices are printed on new paper instead of reused paper containing a customer's information; (c) the delivery man to check the invoices to ensure that the back of the invoices do not contain other customers' information; (d) the acknowledgment copy of the invoices to be destroyed after the delivery man returns the copy to the Organisation; and (e) the Organisation's customer information to be kept safe. The Organisation claimed that some of the policies set out in the document had already been implemented prior to November 2016.

8 The Organisation admitted that none of its staff had undergone any training in respect of the Organisation's obligations under the Personal Data Protection Act 2012[1] ("PDPA"). Further, no training was conducted to explain the Organisation's own internal policies and guidelines to its staff. However, the Organisation claimed that management had briefed staff on the internal policies and guidelines at an unspecified meeting.

1 Act 26 of 2012.

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS AND ASSESSMENT

### *There was unauthorised disclosure of personal data*

9 The information disclosed by the second invoice is personal data within the meaning of s 2 of the PDPA, which requires that the individual may be identified from the data. Given that the surname of the customer was provided, along with the customer's address, e-mail address, and telephone number, it was possible to identify that customer solely from the information disclosed by the second invoice.

10 Given that the disclosure of such information contained in the second invoice was made without consent or authority under the PDPA (or other written laws), it was an unauthorised disclosure of personal data under the PDPA.

### *Unauthorised disclosure was result of breach of the Organisation's obligation to make reasonable arrangements for protection of personal data*

11 The Organisation claims that the unauthorised disclosure was an isolated incident that occurred due to the negligence of its staff. Specifically, that someone accidentally placed the second invoice in the printing tray instead of destroying it. In this regard, it could be argued that the unauthorised disclosure was simply caused by a one-off mistake by the Organisation's staff, and not due to any lack or failure to put in place "reasonable security arrangements" under s 24 of the PDPA.

12 From the Commission's investigations, though, there were more deep-rooted problems with the Organisation's processes, and it lacked the necessary policies and practices to protect personal data. These failures and omissions by the Organisation are detailed below.

#### *The Organisation effectively did not have any policy in place to protect personal data*

13 The Organisation had produced to the Commission a copy of its data protection policy which it says was put in place in November 2016. This is the same month in which the data breach had taken place. Prior to this, the

Organisation claims it did not have a written policy on the protection of personal data.

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.

15 In relation to the Organisation's data protection policy itself, it consisted of a mere six bullet points. At least three of the six points in the policy relate coincidentally to the data breach incident – for example, it provides that the supervisor has to check that the invoices are printed on new paper instead of reused paper containing customer information. Additionally, the policy was put in place the same period of time as the data breach incident. The combination of the timing and content of the policy raises suspicion, and the Commission cannot rule out the possibility, that it was created subsequent to the breach to address that particular incident.

16 Additionally, investigations did not reveal any evidence to show that steps were taken to implement the data protection policy that the Organisation had put in place. Some of the evidence that ought ordinarily to have been presented would be internal communications of the data protection policy to staff, internal briefings conducted to raise staff awareness and training events and collateral to educate staff. During the investigation, the Commission specifically asked the Organisation what other arrangements, apart from the policy documents that they had already produced, the Organisation had in place to mitigate the risk of an unauthorised disclosure of personal data on the printed invoices. The Commission also asked for documentary evidence of such arrangements. The Organisation replied that it had assigned "a supervisor" to ensure that signed invoices were destroyed at the end of each business day, and even suggested that the supervisor was there to check that "invoices were not printed on the reverse side of invoice paper". However, there were several issues which cast doubt on the Organisation's response:

(a) the Organisation did not produce any documentary or other proof of its processes and workflow to show the supervisor's place and role in the relevant process or workflow;

(b) likewise, there was no indication of the actions or tasks that the supervisor was supposed to perform as part of the supervisory checks in the overall invoice process; and

(c) there was no explanation why the supervisor did not pick up on the erroneous invoices (when that was the precise risk that the supervisor was tasked to spot).

In the premises, the Commission assessed the Organisation's claim that it had an effective supervisory check put in place as no more than a bare assertion that was not adequately supported by facts disclosed during investigations. In the final analysis, the Commission is not satisfied by the Organisation's response that the Organisation had translated its policies (if any) to effective practices to protect personal data.

17 From the above, given the shortcomings in the Organisation's data protection policy, and the absence of evidence of its implementation, the Commission is not satisfied that the Organisation had an *effective* data protection policy at the time of the data breach incident to protect personal data.

18 Next, the Organisation admitted that it did not provide any data protection training whatsoever to its employees. Again, staff training forms part of the effective measures to protect personal data. The Commission has emphasised the importance of training in its Advisory Guidelines,[2] and also in its decision in *Re National University of Singapore*.[3] The Commission agrees with the view expressed by the Office of the Australian Information Commissioner: "Regular staff training, and a culture of privacy awareness are essential to ensure compliance."[4]

---

2 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 15 July 2016) at para 17.5.

3 [2018] PDP 155 at [21]–[28].

4 Office of the Australian Information Commissioner, *Introduction to the APPs and OAIC's Regulatory Approach* (May 2005) <https://www.oaic.gov.au/agencies-and-organisations/training-resources/introduction-to-the-apps-and-the-oaic-s-regulatory-approach> at p 24.

19 Overall, it is clear that the Organisation did not make reasonable security arrangements for the protection of personal data:

(a) the Organisation's data protection policy was formalised during the month that the data breach occurred and could have been formalised after the unauthorised disclosure took place;

(b) there was no evidence to show that steps had actually been taken to implement such policy prior to the breach; and

(c) further, the Organisation admitted that its staff had no training whatsoever regarding their data protection obligations.

*At a more basic level, the Organisation did not seem to engage in the issue of what it should do to protect personal data; it had simply relied on its employees carrying out their jobs correctly*

20 A further point must be made. Based on the Organisation's representations, it would appear that the Organisation is essentially relying on its employees and staff carrying out their job functions correctly to say that this is a form of data protection measure in and of itself. If the employees and staff had printed and sent the correct invoice to the correct recipient, there would not be any data protection issue to begin with.

21 In the Commission's view, it is not enough for the Organisation to simply rely on its staff and employees to carry out their duties correctly for the protection of personal data. An organisation has certain obligations with respect to personal data that it has collected and which it holds or has control over. One such obligation is to put in place policies and measures to protect the personal data and to prevent unauthorised use, disclosure or alteration. Policies pertinent and adapted to the Organisation's business and processes ought to be crafted and disseminated to staff. Indeed, s 12(*c*) of the PDPA imposes an obligation for such policies and practices to be communicated to staff. An effective mode of communication is to provide training to staff, whether in traditional classroom settings or through other means such as online training.

22 Crucially, it is important for the management of a company to "buy-in" to adopting good data protection practices for the company. It is from this starting point – the management level – that the company's policies and practices be formulated with data protection in mind. From there, such good data protection policies and practices can permeate down to and be adopted at the staff level of the company. The Commission agrees with the

observation made by the Australian Information Commissioner and Privacy Commissioner of Canada in the joint investigation into *Ashley Madison*:[5]

> Having documented security policies and procedures is a basic organizational security safeguard, particularly for an organization holding significant amounts of personal information. Making informational policies and practices explicit provides clarity about expectations to facilitate consistency, and helps to avoid gaps in security coverage. It also sends key signals to employees about the importance placed on information security. Furthermore, such security policies and processes need to be updated and reviewed based on the evolving threat landscape, which would be very challenging if they are not formalized in some manner.

23 The above position also stresses the importance of having documented policies, as mentioned at [14] above.

24 It is also important that management actively supervises employees and takes responsibility for creating a culture of security-awareness. As observed by the Hong Kong Privacy Commissioner for Personal Data:[6]

> With sound security policies and procedures in place, there is no guarantee that they will be followed. In this regard, supervision and monitoring of the implementation of the procedures are important.

25 Similarly, in its investigation into *Monarch Beauty Supply*,[7] the Office of the Alberta Privacy Commissioner found that the Store Manager and District Manager of the organisation had not been diligent, as they had simply assumed that employees would shred documents containing customers' credit and debit card information, in line with the organisation's policies. However, as management had not provided sufficient instruction

---

5 *PIPEDA Report of Findings #2016-005: Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/ Acting Australian Information Commissioner* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/> at [65].

6 *Investigation Report: Hong Kong Police Force's Repeated Loss of Documents Containing Personal Data* (R13 – 0407) <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R13_0407_e.pdf> at [38].

7 *Order P2006-IR-003: Monarch Beauty Supply [a division of Beauty Systems Group (Canada) Inc]* <https://www.oipc.ab.ca/media/127842/P2006-003IR.pdf> at [40(2)].

on the care and disposal of sensitive documents, the employees in fact threw the documents into the dumpster, which resulted in customers' personal data falling into the hands of criminal suspects. *Monarch Beauty Supply* is an example of what could go wrong and the harm that results from disclosure of personal data due to insufficient follow through on the part of management. The Commission therefore highlights that management has an obligation to establish the standard of care that it expects staff to observe, communicate and train staff, and to put in place appropriate supervision and monitoring to ensure compliance.

26 In this case, for the reasons mentioned above, the Organisation did not have in place, whether at the management or staff level, the necessary policies to protect personal data. It has therefore failed in its obligation to protect personal data under s 24 of the PDPA.

## ENFORCEMENT ACTION BY PERSONAL DATA PROTECTION COMMISSION

27 Given that the Organisation breached its obligation under s 24 of the PDPA, the Commission is empowered under s 29(1) of the PDPA to issue such directions as it thinks fit in the circumstances.

28 The Commission has decided to issue the following directions to the Organisation:

(a) to review its policy for the protection of personal data in relation to its order fulfilment process;

(b) to develop procedures to ensure effective implementation of its data protection policy; and

(c) to conduct training to ensure that its staff are aware of, and will comply with, the requirements of the PDPA when handling personal data.

29 The following mitigating factors were taken into account in arriving at this decision:

(a) the unauthorised disclosure was made to a single person only;

(b) the personal data disclosed were not sensitive; and

(c) there was no evidence that any loss or damage was caused by the unauthorised disclosure.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re Exceltec Property Management Pte Ltd and others

## [2018] PDP Digest 184

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1607-B0117
**Decision Citation**: [2018] PDP Digest 184; [2017] SGPDPC 8

***Application of other written laws*** *– Building Maintenance and Strata Management Act – Consent and notification obligations*
***Consent Obligation*** *– Duration of disclosure of personal data*
***Consent Obligation*** *– Extent of disclosure of personal data – Personal data in minutes of meetings*
***Consent Obligation*** *– Manner of disclosure of personal data – Disclosure on multiple notice boards*
***Consent Obligation*** *– Publicly available data*

12 June 2017

### BACKGROUND

1 This decision arises from three separate cases involving Management Corporation Strata Titles ("MCSTs") and managing agents (collectively "Organisations") of condominiums posting documents containing the personal data of subsidiary proprietors (hereinafter referred to as "residents") on notice boards. The nature of the complaints was that the disclosures made of these personal data was an infringement of the Personal Data Protection Act 2012[1] ("PDPA").

2 The Personal Data Protection Commission ("Commission") commenced investigations into the matter, and provides its decision below.

3 Although the three cases involve different residents and managing agents of condominiums, the facts of the three cases are substantially similar

1 Act 26 of 2012.

and the legal issues involved are identical. Therefore, this consolidated decision is issued for the three cases.

## MATERIAL FACTS AND DOCUMENTS

4 Between 29 June and 27 July 2016, the Commission received complaints from several residents of three condominiums (namely, (a) Prive; (b) The Mornington; and (c) Seletaris) against the condominiums' respective MCSTs or managing agents, namely, (a) Exceltec Property Management Pte Ltd ("Exceltec"); (b) Management Corporation Strata Title Plan No 2956 ("MCST 2956"); and (c) Strata Land Property Consultants Pte Ltd ("Strata Land") respectively:

(a) In the first case, three residents ("First Complainants"), complained that Exceltec had posted copies of the voter list, containing the names, unit numbers and voting shares of residents, and the draft minutes of the first council meeting on 12 July 2016 (containing the names and unit numbers of residents) on notice boards of the Prive condominium and Prive EC web portal without providing prior notification and obtaining their consent.

(b) In the second case, a resident ("Second Complainant"), complained that MCST 2956 had left the voter list, containing the names and unit numbers of residents, on a publicly accessible notice board for longer than necessary after the conclusion of the annual general meeting. According to the Second Complainant, the voter list was left on the board for roughly two months after the council meeting was held.

(c) In the third case, a resident ("Third Complainant"), complained that Strata Land had posted a voter list, containing the names, unit numbers and voting shares of residents, on at least two notice boards at different blocks of the Seletaris condominium. The Third Complainant alleged that there was no need to have posted the voter list on multiple notice boards, and further, that the voter lists had been displayed for an unnecessarily long period of time (*ie*, two days after the council meeting).

5 For ease of reference, we set out in a table below a summary of the types of personal data that were disclosed by the Organisations and the nature of the complaints that were made by the various complainants.

| No | Relevant parties | Documents Involved | Personal Data Involved | Nature of Complaint |
|---|---|---|---|---|
| 1. | First Complainants<br>Exceltec | (a) Draft minutes of meeting<br>(b) Voter list | (a) Names and unit numbers<br>(b) Names, unit numbers and voting shares | Disclosure of personal data without notification or consent. |
| 2. | Second Complainant<br>MCST 2956 | Voter list | Names and unit numbers | Duration of the disclosure of personal data was for longer than necessary. |
| 3. | Third Complainant<br>Strata Land | Voter list | Names, unit numbers and voting shares | Disclosure of personal data without notification or consent.<br>Duration of the disclosure of personal data was for longer than necessary.<br>Disclosure of personal data ought not to be made on multiple notice boards. |

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS AND ASSESSMENT

### *Applicability of the Personal Data Protection Act*

6 The posting of the voter lists and minutes of meeting by the Organisations on notice boards located within the compound of the condominiums amounted to a "disclosure" under the PDPA of the information in the voter list and minutes of meeting.

7 As seen in the table above, the information that was disclosed in the voter lists and minutes of meeting included the names, unit numbers and voting shares of the residents. This information constitutes "personal data" under s 2(1) of the PDPA because the residents could be identified from such information. For example, the Second Complainant could be identified from the voter list that MCST 2956 had disclosed on The Mornington's notice board, which included the name, unit number and voting shares of the Second Complainant.

8 Given that the disclosed information constitutes personal data, the Organisations are therefore subject to the data protection provisions in Pts III–IV of the PDPA in relation to the disclosure of that personal data.

### *Issues to be determined*

9 There are two data protection obligations under the PDPA that are relevant to the disclosures that were made by the Organisations – the consent obligation[2] ("Consent Obligation") and notification obligation[3] ("Notification Obligation").

(a) The Consent Obligation generally requires organisations to obtain consent from an individual for the collection, use or disclosure of his or her personal data.

(b) The Notification Obligation generally requires that notice of the purposes for which organisations collect, use or disclose personal data be given to the individual beforehand.

10 Both the Consent and Notification Obligations are subject to various exceptions under the PDPA, including the exceptions found in the Second to Fourth Schedules to the PDPA. Additionally, s 4(6) of the PDPA allows the provisions of other written law to prevail over data protection obligations where they are inconsistent with the provisions of that other written law ("the subordination provision").

11 The first issue is therefore whether the Organisations have complied with the Consent and Notification Obligations, or whether they can avail themselves of any exceptions under the PDPA.

12 For this issue, we will examine what the Commission considers is the crux of the matter: (a) whether, by reason of the subordination provision, the requirements for Organisations to notify and obtain consent to disclose the voter lists and minutes of meeting containing personal data are superseded by the Building Maintenance and Strata Management Act[4] ("BMSMA") requirements for such voter lists and minutes of meeting to be disclosed; and/or (b) whether the public availability exception applies.

---

2 Pursuant to ss 13–15 and 17 of the Personal Data Protection Act 2012 (Act 26 of 2012).

3 Pursuant to s 20 of the Personal Data Protection Act 2012 (Act 26 of 2012).

4 Cap 30C, 2008 Rev Ed.

13 The second issue is whether, even if the disclosure was permissible in respect of the first issue above, the Organisations had disclosed more personal data than what was permitted in the voter lists and minutes of meeting.

14 The final two issues are: (a) whether MCST 2956 and Strata Land had disclosed the personal data for a longer duration than necessary; and (b) whether Strata Land was permitted to disclose the voter lists on multiple notice boards located in the condominium.

### *Issue (a): Whether the Organisations had obtained consent or provided notification when they disclosed personal data of residents*

15 As part of the Consent Obligation, s 13 of the PDPA requires that prior consent be obtained by an organisation in order to collect, use or disclose personal data about an individual.

16 This is concomitant with the Notification Obligation, which requires, under s 20 of the PDPA, that notification be provided to the individual of the purposes for the collection, use or disclosure of personal data before consent is obtained. However, the need to obtain consent or to provide the related notification is dispensed with where an exception to s 13 of the PDPA (*ie*, the Consent Obligation) applies.

17 Based on the Organisations' representations to the Commission, none of the Organisations had notified their respective residents of the purpose of the disclosure of the voter lists or minutes of meeting, nor did any Organisation obtain the residents' consent to disclose their personal data.

18 Accordingly, the next question is whether the Organisations could avail themselves of an exception to s 13 of the PDPA (*ie*, the Consent Obligation).

### *Issue (b): Whether disclosure may be made without consent*

#### *Sub-issue (1): Whether disclosure was required or authorised under other written law*

19 Section 13(*b*) of the PDPA provides for an exception to the need for consent to be obtained – it states that an organisation shall not disclose personal data unless the disclosure without the consent of the individual is

required or authorised under the PDPA or any other written law. Simply put, in so far as there is another written law which requires or authorises the disclosure of personal data, an organisation which does so pursuant to that law will be able to avail itself of the exception under s 13(*b*) of the PDPA. In the present case, the other written law in question is the BMSMA.

20 Under para 7 of the First Schedule to the BMSMA, management corporations are statutorily required to display a list of voters entitled to vote at the general meeting on the notice board maintained on the common property. Paragraph 7 of the First Schedule to the BMSMA reads as follows:

> **List of names of persons entitled to vote**
> 7. The secretary of the management corporation or (as the case may be) subsidiary management corporation *shall put up a list of the names of the persons who are entitled to vote at a general meeting on the notice board maintained on the common property* at least 48 hours before the general meeting.
>
> [emphasis added]

21 The BMSMA therefore requires that the names of the persons entitled to vote at the general meeting be put up on the notice board. It does not, however, state that other information, namely, the unit numbers or voting shares, may also be disclosed in the voter list. This would be an issue which we will address further below at [30]–[39].

22 Similarly, management corporations are required under para 3 of the Second Schedule to the BMSMA to keep the minutes of any meeting of the council or executive committee of the management corporation, and display those minutes on the notice board. Paragraph 3 of the Second Schedule to the BMSMA reads as follows:

> **Keeping of records**
> 3.—(1) The council or executive committee shall keep minutes of its proceedings and shall cause minutes of general meetings to be kept.
> (2) If the management corporation or subsidiary management corporation is required by its by-laws to maintain a notice board, its council or executive committee, as the case may be, shall —
>
> (*a*) *cause a copy of the minutes of a meeting of the council or executive committee, as the case may be, to be displayed on the notice board within 7 days after the meeting*; and
>
> (*b*) cause a copy of a minute of any resolution thereof, or of the management corporation or subsidiary management corporation, as

> the case may be, passed in accordance with this Act to be displayed on the notice board after it is passed.
>
> (3) A copy of any minutes referred to in sub-paragraph (2) shall be kept displayed on the notice board for a period of not less than 14 days.
>
> (4) If there is no notice board, the council or executive committee concerned shall give each resident a copy of the minutes referred to in sub-paragraph (2)(*a*) or (*b*) within the period specified in that sub-paragraph.
>
> (5) The council or executive committee shall —
>
> (*a*) cause proper books of account to be kept in respect of all sums of money received and expended by it, specifying the matters in relation to which the receipts and expenditure take place; and
>
> (*b*) on the application of a resident or mortgagee of a lot (or any person authorised in writing by him), make the books of account available for inspection at all reasonable times.
>
> [emphasis added]

23 While para 3 of the Second Schedule to the BMSMA does not expressly state the information that ought to be included (or omitted) in the minutes of meeting that is displayed on the notice board, in the Commission's view, the function and purpose of minutes of meetings, at least in the context of the BMSMA, is to fully and accurately record what was discussed and what happened at the meeting. This includes recording the declarations made under s 60(7) of the BMSMA,[5] and the resolutions and/or motions that were passed. Such minutes serve a variety of purposes including being a record of discussions for future reference, or to capture the rationale behind the decisions being made. It is therefore *implicit* in the definition and understanding of "minutes of meetings" that it can contain the personal data of individuals, as part of this full and accurate recording of the meeting: *eg*, attendance, participation in discussions and views expressed, as the subject of matters discussed in the meeting agenda.

---

5 Section 60(7) of the Building Maintenance and Strata Management Act (Cap 30C, 2008 Rev Ed) states: "The secretary of the council shall record every declaration under this section in the minutes of the meeting at which it was made."

24 In this regard, the Commission agrees with the position taken by the Office of the Information and Privacy Commissioner of British Columbia ("OIPC"):[6]

> [A] strata council should ensure that every statement in the strata council minutes is accurate, objective and verifiable and that the minutes contain the minimum amount of personal information necessary.

25 The OIPC also provided some guidance on the personal information that may be recorded in the strata council minutes:[7]

> If a strata council member or a guest attends a strata council meeting, they have provided implied consent to have their name recorded in the strata council minutes.
>
> Similarly, the names of any authorised people in attendance at the meeting, such as the strata manager, can be noted in the minutes. The name, strata lot number and/or unit number of each strata council member, who is not attending the meeting, should also be recorded.
>
> …
>
> Minutes of strata council meetings should record all decisions made by the strata council, but need not include the exact discussions leading up to any votes. It is important that the strata council minutes clearly document how resolutions are amended and what the outcome of any votes were.
>
> Strata councils should ensure that only the minimal amount of personal information required to provide an accurate and objective account of its decisions is recorded in the meeting minutes.

26 In the Exceltec case, the draft minutes of the first council meeting disclosed the names and unit numbers of the residents. In the Commission's view, the names of the residents would reasonably form part of the minutes of the council meeting as there is a need to identify and record the persons in attendance (or absence), including the council office bearers and the residents who are sitting in the meeting as observers. Given that para 3 of the Second Schedule to the BMSMA provides for an

---

6 Office of the Information and Privacy Commissioner of British Columbia, *Privacy Guidelines for Strata Corporations and Strata Agents* (June 2015) <https://www.oipc.bc.ca/guidance-documents/1455> at p 19.

7 Office of the Information and Privacy Commissioner of British Columbia, *Privacy Guidelines for Strata Corporations and Strata Agents* (June 2015) <https://www.oipc.bc.ca/guidance-documents/1455> at p 17.

organisation (specifically, the MCST or managing agent) to disclose the full and accurate minutes of the council meeting on the notice board, it must be taken that the personal data (*ie*, the names) are to be disclosed as part of the overall publication of the minutes of meetings. When read together with s 13(*b*) of the PDPA, Exceltec is allowed to disclose the names of the residents in the minutes of meeting without obtaining the residents' consent.

27 In respect of the unit numbers found in the minutes of meeting, it should first be noted that a unit number in and of itself is not personal data. The association of the unit number with the person attending the meeting renders the pair personal data. Having considered the matter, the Commission is of the view that if the purpose of including the name of the person attending the council meeting is to identify him, then the inclusion of the unit in the minutes of meeting is reasonable because it serves to establish the basis for his attendance (*ie*, he is the subsidiary proprietor or represents the subsidiary proprietor of that unit). In any event, as will be dealt with below, the publicly available exception would apply to the disclosure of such personal data.

28 In light of the foregoing, the Commission makes the following findings:

(a) In respect of the disclosures that were made by the Organisations of the residents' names in the voter lists, these were in compliance with the Consent Obligation and Notification Obligation, pursuant to para 7 of the First Schedule to the BMSMA read with s 13(*b*) of the PDPA.

(b) In respect of the disclosures of the residents' (i) names and (ii) unit numbers that were made by Exceltec in the minutes of meetings, these were in compliance with the Consent Obligation and Notification Obligation, pursuant to para 3 of the Second Schedule to the BMSMA read with s 13(*b*) of the PDPA.

29 This leaves open the question of whether or not the disclosures of (a) unit numbers and (b) voting shares of residents in the voters list are also permitted to be disclosed under the PDPA. These two issues will now be addressed in the paragraphs below.

*Sub-issue (2): Whether disclosure fell under public availability exception*

30 The Commission also found that the public availability exception[8] is applicable in this case. Public availability (of the personal data) is an exception to the Consent Obligation and Notification Obligation, and allows for personal data to be disclosed without obtaining consent, as provided for in s 17(3) of the PDPA read with para 1(*d*) of the Fourth Schedule to the PDPA.

31 Public availability, in relation to personal data about an individual, is defined in s 2(1) of the PDPA to be personal data that are generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or event (a) at which the individual appears and (b) that is open to the public.

32 In its *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, the Commission has stated at para 12.58 that personal data will be generally available to the public as long as "any member of the public could obtain or access the data with *few or no restrictions*" [emphasis added].

33 In the present case, the disclosures that were made by the Organisations, on the whole, were the (a) names, (b) unit numbers and, in the cases of Exceltec and Strata Land (c) the voting shares of residents. The Commission is of the view that all these three types of personal data were generally available to the public for the following reasons.

34 First, the information can be found in the strata roll, which is generally available to the public. Under s 47(1)(*b*) of the BMSMA, any resident or mortgagee, prospective purchaser or mortgagee, or even a person authorised in writing by the resident or mortgagee, may make an application to the managing corporation for the property's strata roll. All management corporations are required to prepare and maintain a strata roll which contains, among other things, (a) the names and (b) the addresses (including the apartment unit number) of residents and mortgagees of the lots, and (c) the respective share value of the lots.[9] Since access to these

8 Personal Data Protection Act 2012 (Act 26 of 2012) Fourth Schedule, para 1(*d*).

9 Pursuant to s 46 of the Building Maintenance and Strata Management Act (Cap 30C, 2008 Rev Ed).

strata rolls extends to "prospective" purchasers or mortgagees as well, in practical terms, this allows almost any member of public who claims to be a "prospective" purchaser to gain access to the information in the strata roll.

35 Second, there are few restrictions under the BMSMA for a person to gain access to the strata roll. In order for a person to inspect the strata roll (amongst other information that the MCST has to make available under s 47(1)(*b*) BMSMA, *ie*, minutes of general meetings of MCST and council, or any other record in the custody or control of the MCST), the person only needs to do two things: (a) make an application to the MCST and (b) pay the prescribed fee in order to obtain the strata roll. There are generally no other prerequisites or qualifications needed to fulfil in order to obtain the strata roll. Even though s 47 of the BMSMA states that the strata roll shall only be made available to a defined group (*ie*, residents, mortgagees or purchasers), "prospective" mortgagees or purchasers as well as such persons authorised by residents or mortgagees are included in the group. The expansion of the defined group renders it very difficult to enforce checks to ensure that the applicant for the information falls within the class. The practical reality is that there is a very low barrier to cross for a person to access the strata roll, besides just simply making the online application and paying the prescribed fee.

36 Third, some of this information may already be found on the Singapore Land Authority Registry ("SLA"), which the public would generally have access to. In this regard, anyone can purchase property title information, property ownership information and land information, which include name, unit number and share value of the lot, for a prescribed fee. Similar to the strata roll, SLA imposes no or few restrictions on the purchase.

37 Accordingly, the Commission takes the view that the names, unit numbers and voting shares of the residents (which are, for all intents and purposes, the same as the share value of the apartment) are publicly available information under the PDPA.

38 As the information was publicly available, therefore, pursuant to s 17(3) of the PDPA and para 1(*d*) of the Fourth Schedule to the PDPA, there was no need for the Organisations to obtain consent from the residents or provide prior notification to the residents before the Organisations disclosed the names, unit numbers and voting shares of the residents found in the strata rolls.

39 In light of the above, the Commission is of the view that the above exceptions are applicable, and that the Organisations are neither in breach of the Consent Obligation nor the Notification Obligation in respect of the residents' personal data.

### *Issue (c): Whether the Organisations had disclosed more personal data than necessary in voter lists and minutes of meeting*

40 In consideration of the applicability of the exceptions to the PDPA, the Commission also looked at whether the Organisations had disclosed more personal data than they were required or authorised to in the voter lists and minutes of meeting.

#### *Voter lists*

41 It was already determined above that the Organisations are permitted to disclose the names of residents for the voter list on the notice board, without obtaining consent or providing notification, pursuant to para 7 of the First Schedule to the BMSMA and s 13(*b*) of the PDPA.

42 However, based on the express wording of para 7 of the First Schedule to the BMSMA, this does not appear to extend to the disclosure of unit numbers and voting shares of the residents. The exception under s 13(*b*) of the PDPA therefore does not apply to the disclosure of such personal data on the notice board.

43 Nonetheless, as mentioned above, the residents' unit numbers and voting shares were publicly available information, and therefore could be disclosed without notifying the residents of the purpose for disclosure or obtaining prior consent from them before disclosure.

#### *Minutes of meeting*

44 Turning to the minutes of meeting, the Commission also considered whether Exceltec was specifically required to record the personal data of the residents, *ie*, their names and unit numbers, in the draft minutes of the first council meeting.

45 It has already been mentioned above at [26]–[28] that personal data found in the minutes of meetings may be disclosed pursuant to para 7 of the First Schedule to the BMSMA read with s 13(*b*) of the PDPA.

46 However, this position should not be construed to mean that MCSTs and managing agents may include personal data of their residents without any restriction. The Commission cautions that any personal data recorded in the minutes should be relevant to the proceedings and necessary to ensure a full and accurate record of the conduct of the meeting. In a case where personal data are disclosed without being in any way relevant to the agenda of the meeting, the Commission may take the appropriate enforcement action.

### *Issue (d): Whether the Organisations had disclosed personal data for longer than necessary*

47 Keeping the voter lists posted on the notice boards for a period of time may be seen as a continuous disclosure of the personal data in the voter lists. In the case of Strata Land, the disclosure was for approximately a two-month period, whereas in the case of MCST 2956, the disclosure was for a two-day period.

48 The Commission is of the view that MCSTs and managing agents should generally keep the voter list and minutes of meetings that contain personal data on the notice board only for a reasonable period of time. Good data protection practices dictate that the period of exposure of personal data and the length of such exposure should be minimised as far as possible, even if the disclosure is, in and of itself, permitted under the PDPA. By keeping personal data longer than necessary, an organisation runs the risk of falling afoul of the retention obligation under s 25 of the PDPA.

49 In the case of MCST 2956, displaying the voter list on the notice board for two days cannot be said to be unduly protracted. In the case of Strata Land, the period was two months. Considering that the voter list is intended to establish both the persons who are entitled to attend and vote at the meeting and also the share value or voting rights of each of such persons, it stands to reason that the voter list may be displayed on the notice board for as long a duration as the minutes of meeting. This provides the conscientious reader of the minutes of meeting the means by which to verify the accuracy of the minutes of meeting, in so far as it concerns the identity of the voters and the calculation of votes. The Commission bore in mind that the minutes of meeting must be displayed for at least 14 days: see para 3 of the Second Schedule to the BMSMA, reproduced at [22] above.

50 Taking this minimum period of displaying as the basis for comparison, it is the Commission's view that keeping the voter list posted on the notice board for two months is not an unduly protracted period. Admittedly, assessments of discretions are not an exact science and there can be a range of validly held views as to what a reasonable period ought to be. In cases such as these where the reasonableness of a course of action is called to question, the Commission restricts its role to determining when the action is so clearly unreasonable such that sanctions under the PDPA are warranted. For the present case, it is not necessary to express any view as to when a period crosses the threshold and becomes unreasonably protracted. It is sufficient for this decision that a period of two months is not so unreasonably long that it ought to attract a sanction under the PDPA.

51 In this case, for the reasons above, the Commission finds that MCST 2956 and Strata Land are not in breach of the PDPA in respect of the duration of the disclosures that were made.

### *Issue (e): Whether disclosure of personal data may be made on multiple notice boards*

52 The last issue, raised by the Third Complainant, is whether there was a requirement that the disclosure of the voter lists had to be made on all the notice boards of the condominium unit, or whether it was only necessary for the disclosure to be made on one.

53 Since the disclosure of personal data in the voter list is permissible under the PDPA for the reasons above, there are no restrictions to the voter list being disclosed on multiple notice boards under the PDPA. Moreover, the BMSMA does not make a distinction whether or not the disclosure is to be made on one notice board or multiple notice boards.

54 Accordingly, Strata Land is not in breach of the PDPA for disclosing the voter list on multiple notice boards.

## CONCLUSION

55 For the foregoing reasons, the Commission therefore concludes that the Organisations have not breached the Consent and Notification Obligations under the PDPA in relation to the disclosure of personal data

in the voter lists and minutes of meeting, and has decided to take no further action in respect of the complaints made.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re Hazel Florist & Gifts Pte Ltd

## [2018] PDP Digest 199

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1609-B0194
**Decision Citation**: [2018] PDP Digest 199; [2017] SGPDPC 9

***Protection Obligation*** *– Disclosure of personal data – Insufficient security arrangements*

20 June 2017

### BACKGROUND

1 The organisation ("Organisation") is incorporated in Singapore and is in the business of, amongst other things, selling and delivering gift hampers. Sometime in August 2016, the Organisation delivered a gift hamper to the complainant ("Complainant"). The Complainant on unwrapping the gift hamper discovered that order forms ("Order Forms") were used as fillers to cover the bottom of the hamper he received ("Incident"). The personal data of other individuals were clearly visible on these Order Forms. The Complainant complained of this disclosure of personal data by the Organisation to the Personal Data Protection Commission ("Commission") on 5 September 2016.

2 Based on the complaint that was made, the Commission proceeded to investigate if there was a breach of the Organisation's obligations under the Personal Data Protection Act 2012[1] ("PDPA") by the disclosure to the Complainant. The following sets out the Commission's findings following its investigations into the matter.

1 Act 26 of 2012.

## MATERIAL FACTS

### *Gift hamper packing process – Order Forms were not designated as "fillers"*

3 Employees in the Organisation's Production Department ("Production Employees") are responsible for packing the gift hampers. The Production Employees cover the bottom of the hampers with "fillers". The materials used as fillers ("Designated Filler Material"), which include loose paper strips and shredded newspapers, outdated brochures and flyers, are kept in an allocated area near the Production Employees. The Designated Filler Material is replenished by the employees according to a roster. Order Forms were not Designated Filler Material.

### *Production Employee uses Order Forms meant for disposal as she runs out of Designated Filler Material*

4 Employee Y, a recent hire who was only on the job for about a month, was tasked to pack the Complainant's gift hamper. The Designated Filler Material kept at the allocated area had run out while Y was wrapping the Complainant's gift hamper. Y took the Order Forms which were placed in a box within the Production Department's workspace and used them as fillers for the Complainant's gift hamper instead. The Order Forms in this box relate to orders for gift hampers or floral bouquets that the Production Department had already packed or arranged; these Order Forms were meant to be disposed of. The box containing these Order Forms was easily accessible by any of the Organisation's employees.

### *Complainant's gift hamper passes quality control check and is delivered*

5 Once Y finished packing the Complainant's gift hamper, another employee tasked to perform quality control checks ("QA Employee") ensured that the hamper contained the items ordered by visually comparing the items in the Complainant's gift hamper against the relevant order form in accordance with the usual process. These quality control checks are to ensure that the items packed in the gift hampers match the items stated in the relevant Order Forms and not for checking what filler material was used. In any event, it would have been impossible for the QA Employee to

check what filler material was used for the Complainant's gift hamper as the filler material was covered with an opaque sheet.

6 The gift hamper was delivered to the Complainant and as a result personal data of approximately 24 unique individuals written or printed on the Order Forms were disclosed to the Complainant.

7 The personal data ("Personal Data") visible in the Order Forms were the names, delivery addresses and telephone numbers of the recipients and the reasons the gift hampers were ordered for the recipients (*eg*, birth of a child or as wishes for a speedy recovery). In one instance, the National Registration Identity Card ("NRIC") number of a recipient was shown on one of the disclosed Order Forms.

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

### *Elements of section 24 obligation under the Personal Data Protection Act*

8 Based on its investigations, the Commission finds the Organisation in breach of s 24 of the PDPA as it:

(a) is an organisation within the meaning of the PDPA;
(b) is in possession or control of the Personal Data; and
(c) did not make reasonable security arrangements to prevent the unauthorised disclosure of the Personal Data.

9 The first two elements are preconditions to the application of s 24 of the PDPA; the obligation to make reasonable security arrangements does not attach unless elements (a) and (b) are present. It is clear from the facts that the preconditions are met and that s 24 of the PDPA applies to the Organisation. The Organisation does not dispute that s 24 of the PDPA applies in this matter. This grounds of decision, therefore, only sets out the Commission's findings on the third element (whether reasonable security arrangements were made). The Commission's reasons for finding that the Organisation did not make reasonable security arrangements to prevent the unauthorised disclosure of the Personal Data are set out below.

***The Organisation did not implement any measures to ensure that its employees only used Designated Filler Material***

10 The Organisation did not anticipate the unauthorised disclosures in this Incident as it believed that its employees would not use materials other than the Designated Filler Material to pack gift hampers. This is clear from the Organisation's response to the Commission's request for an account of the Incident. In its official response, the Organisation states that:

> In hazel, we have a clear procedure on what materials that has to be used for the packaging, and basing from what had transpired, the staff has clearly broken our guidelines that resulted to this unacceptable error, we have to point out that *it should have been impossible for any our staff to use any of those documents because its not even considered a packaging material* … [emphasis added]

11 The procedure referred to in the Organisation's response above is that Production Employees were instructed to use the Designated Filler Material found in the allocated area for packing gift hampers.

12 However, the Organisation's instruction to its employees to use the Designated Filler Material for packing gift hampers is not in itself a reasonable security arrangement. The protection obligation in s 24 of the PDPA obliged the Organisation to implement reasonable security arrangements that protected the personal data found in the Order Forms from unauthorised disclosure through Y's use of Order Forms as fillers. The Organisation's instruction to its employees without any accompanying measures reasonably ensuring that the instruction was carried out by its employees does not satisfy the protection obligation.

***Y did not receive any data protection training***

13 It is possible, depending on the specific circumstances, that data protection training may serve as a security arrangement. Any such data protection training should be designed to provide an employee with an awareness of the organisation's data protection obligations and specific guidance on the proper handling of personal data relevant to the employees' day-to-day tasks.

14 In this instance, however, the Organisation did not provide any such data protection training. The Organisation communicated its instruction on the use of Designated Filler Material to its employees through on-the-

job training. This training involved members of the Production Department guiding Y on how to pack the gift hamper. It was not designed to include training on data protection. Merely training an employee on her role does not constitute a security arrangement.

15 This lack of training showed in Y's clear lack of awareness on the importance of data protection; anyone with a basic idea of the importance of protecting personal data would not have used the Order Forms as packing material.

***Y was not properly supervised in her work***

16 Further, the Organisation acknowledged that, after a time, Y was not receptive to the training and guidance provided by her colleagues. Y brushed off her colleagues' attempts to train and guide her through the procedure for packing gift hampers and did not follow instructions. The Organisation failed to address Y's lack of receptiveness to the training.

17 Without the guidance of her team members and the lack of intervention by the Organisation, Y was effectively working unsupervised. Given the Organisation's practices, this lack of supervision meant that the Organisation was practically unable to ensure that Y followed the Organisation's instruction to use the Designated Filler Material.

***The Organisation's data protection policy and employee handbook did not provide specific practical guidance on proper handling of personal data***

18 The Commission notes that the Organisation has in place a data protection policy ("Data Protection Policy"). The Data Protection Policy merely restates the Organisation's data protection obligations in very general terms. The Organisation's Data Protection Policy does not provide the Organisation's employees with specific practical guidance on how to handle personal data in their day-to-day work or how to comply with s 24 of the PDPA. The Commission is, therefore, of the view that the Organisation's Data Protection Policy does not constitute a "security arrangement" under s 24 of the PDPA. In this regard, the Commission

repeats its advice in its decision in *Re National University of Singapore*:[2] "Proper guidance is not easily substitutable or replaceable by general guidelines that an organisation may set."

19 Further, the Organisation merely expects new staff to read the Data Protection Policy on the first few days after commencing employment. The Organisation does not ensure that the Data Protection Policy has been explained to the employees or that the employees understand what is required of them under the policy. Such policies and practices do not constitute a "reasonable security arrangement" under s 24 of the PDPA.

20 The Commission notes that the extract of the Organisation's employee handbook provided to the Commission and titled "Professional Handling of Hazel Florist Confidential Information" does not even address personal data and instead addresses the handling of information that the company holds out to be confidential. The section generally provides that employees are not to "divulge, share any trade and/or sensitive information regarding the business of the company in whatever form or media to unauthorized party or parties".

### *Personal Data Protection Commission's decision: The Organisation is in breach of section 24 of the Personal Data Protection Act*

21 Viewing the circumstances as a whole, the Commission finds the Organisation in breach of s 24 of the PDPA. The Organisation failed to make reasonable security arrangements to protect the Personal Data as:

(a) the Organisation did not implement any measures to reasonably ensure that its instruction to its employees to use the Designated Filler Material to pack gift hampers was carried out by its employees;

(b) the Organisation did not provide Y with any data protection training;

(c) the Organisation failed to ensure that Y was properly supervised in her work;

(d) the Organisation's Data Protection Policy and employee handbook did not provide specific practical guidance on handling personal data or complying with s 24 of the PDPA; and

2 [2018] PDP Digest 155 at [32].

(e) there was no other form of security arrangement in place to protect the Personal Data.

22 This Incident should not have come as a surprise to the Organisation. Given the above, an incident such as this was waiting to happen.

## REMEDIAL ACTIONS TAKEN BY THE ORGANISATION

23 The Organisation has taken the following remedial actions to help prevent the disclosure of personal data found in Order Forms in the future:

(a) reminders not to use documents containing personal data of customers as packaging materials and to only use designated packaging materials have been posted at all employee workspaces;
(b) meetings and group discussions were held with employees to emphasise the above reminders;
(c) limiting access to the box containing Order Forms meant for disposal to only authorised employees by securing it with a lock; and
(d) the Organisation is revising its Order Forms so that the forms will only state the delivery address, the date and time of delivery, and the product code.

## ENFORCEMENT ACTION BY PERSONAL DATA PROTECTION COMMISSION

24 The Commission 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 $1m as the Commission thinks fit.

25 In determining the directions to be imposed on the Organisation, the Commission took into account the following factors:

(a) the Personal Data was disclosed to only one person;
(b) save for the disclosure of one individual's NRIC number, the breach involved personal data of limited sensitivity;
(c) the Organisation has taken remedial actions to help prevent the disclosure of personal data in the future; and
(d) the Organisation has been fully co-operative in the investigation.

26 In view of the factors noted above, the Commission has decided to issue a Warning to the Organisation for the breach of its obligations under s 24 of the PDPA. The Commission is of the view that neither further directions nor a financial penalty is warranted in this case.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re DataPost Pte Ltd

## [2018] PDP Digest 207

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-1606-B0061
**Decision Citation**: [2018] PDP Digest 207; [2017] SGPDPC 10

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

20 June 2017

## BACKGROUND

1 This case arises out of an investigation into DataPost Pte Ltd ("DPL"). DPL printed and mailed out financial statements relating to the Overseas-Chinese Banking Corporation Ltd's ("OCBC") Supplementary Retirement Scheme ("SRS") to OCBC's customers. One customer ("the recipient"), however, discovered that she had received two additional SRS statements belonging to two other OCBC customers, in addition to her own SRS statement. The following information was disclosed in the SRS statements:

(a) name;
(b) address;
(c) cash balance; and
(d) types, quantity and valuation of asset holdings.

2 OCBC alerted the Commission to the incident, and informed the Commission that the recipient had received the additional SRS statements on or about 17 June 2016. The Commission has conducted an investigation into the matter and now sets out its findings.

## MATERIAL FACTS AND DOCUMENTS

3 DPL's procedure for printing and mailing of the SRS statements was as follows:

(a) The SRS statements are printed on A3 sheets in the format shown below. A sheet may contain either two different statements or two pages of the same statement. In the incident in question, the first sheet, Sheet 1, contained the statements of two different individuals. Sheet 2 also contained the statements of two different individuals.

A3 size Sheet 1

| | |
|---|---|
| Statement of Individual 1 | Statement of Individual 2 |

A3 size Sheet 2

| | |
|---|---|
| Statement of Individual 3 | Statement of Individual 4 |

(b) An enveloping machine was used to cut the statements and to insert the individual statements into their respective mailer envelopes. For the purpose of this decision, there are two relevant sub-components of the enveloping machine which operations affect the eventual output of the enveloping machine. These are the cutter, which cuts the sheets of paper into A4 pages; and the optical mark recognition ("OMR") reader that reads OMR markings (which are lines resembling barcodes) that are printed on each customer's statements. The OMR reader guides the enveloping machine to insert each

customer's statements into the mailer envelope intended for that customer.

(c) The enveloping machine was operated by a single operator. The operator would start each printing run with a test run. If the test run was successful, the operator would proceed with the printing and enveloping of the entire batch of statements.

(d) The design of the machine was such that the first sheet, Sheet 1, had to be loaded directly into the cutter. However, the cutter was located further along in the machine than the OMR reader. Therefore, the first two statements cut from Sheet 1 would always be placed by the machine in the same envelope as the first statement of Sheet 2.

(e) As a result of this operational peculiarity, the machine was set to automatically send the first envelope into the reject bin for manual intervention. The operator was supposed to sort out the individual statements in the reject bin by hand and put them into separate envelopes. He was then supposed to leave the sorted statements and envelopes in the reject bin for a quality control ("QC") check by a second level checker.

(f) Having passed the second level check, a *third* check for QC was to be conducted by a supervisor. All three levels of checks were supposed to be recorded in a QC form.

(g) Correctly filled envelopes were supposed to be deposited by the machine in the main bin. There is a digital counter in the main bin that records the number of envelopes deposited into it. The operator was supposed to record this number in the QC form together with the number of rejected envelopes. The number of "successful" and rejected envelopes, when added up, was supposed to tally with the total expected number of envelopes from the run.

4 The cause of the data breach in this case, according to DPL's internal investigations, was human error by the operator on duty on 4 May 2016. DPL's findings were that the operator manually checked the first envelope generated by the test run, but mistakenly concluded that the three statements contained therein all belonged to the same person. In fact, the statements belonged to three separate individuals, and had been placed in the same envelope due to the operating peculiarity described above.

5 The operator, in the mistaken belief that the three statements belonged to the same individual, removed the envelope from the reject bin

and moved it to the main bin. Further, the operator completed the QC form in a way that showed that the number of "successful" and rejected envelopes tallied with the expected total from the run. As the envelope was no longer in the reject bin, the second and third layers of checks were by-passed, and the envelope was sent out without anyone realising that it contained two extra statements. The manual completion of the QC form by the operator to show that the number of successful and rejected envelopes tallied allowed this to go undetected.

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS AND ASSESSMENT

### *There was unauthorised disclosure of personal data*

6 The information disclosed in the two SRS statements is personal data within the meaning of s 2 of the Personal Data Protection Act 2012[1] ("PDPA"). First, the names and addresses of the intended recipients of those two statements were included on the statements themselves. Hence, those individuals could be identified solely from the information disclosed by the statements. Further, the SRS financial information contained therein was clearly their personal data.

7 Given that the disclosure of such information contained was made without the consent of the intended recipients (*ie*, the data subjects), and without any authority under the PDPA (or other written law), it was an unauthorised disclosure of personal data for the purposes of the PDPA.

### *DPL was a data intermediary and had obligation to protect personal data under section 24 of the Personal Data Protection Act*

8 In relation to the printing and mailing of the statements containing personal data, DPL was "processing" personal data under s 2 of the PDPA. As DPL was processing the personal data on behalf of OCBC, pursuant to their service agreement, DPL is a data intermediary within the

1 Act 26 of 2012.

meaning of s 2 of the PDPA: see also, *Re Central Depository (Pte) Limited*[2] and *Re Aviva Ltd*.[3]

9 Hence, as provided under s 4(2) of the PDPA, DPL was under an obligation to make reasonable security arrangements to prevent the unauthorised disclosure of personal data under s 24 of the PDPA in respect of the personal data that DPL was processing for OCBC.

### *Unauthorised disclosure was result of breach of DPL's obligation to make reasonable arrangements for protection of personal data*

10 DPL claims that the unauthorised disclosure was the result of a single instance of human error. DPL provided a written data protection policy to the Commission. This policy states that envelopes in the reject bin should be treated with extra care, and that it was mandatory for such rejected envelopes to be subjected to second and third level checks. Taken together with the steps outlined above, DPL did have in place data protection policies and processes.

11 However, the Commission is of the view that the processes that DPL put in place did not meet the reasonable standards expected of it. There were two main issues in DPL's processes:

> (a) it created a significant risk of the first envelope containing the statements of more than one individual (which may subsequently lead to an unauthorised disclosure of personal data); and
>
> (b) it placed too much reliance on the operator to ensure that the first batch of statements were correctly sorted out and separated into the different envelopes, before sending out. Pertinently, DPL's QC checks were over-reliant on the operator strictly adhering to DPL's procedures, and correctly performing each of his functions, in order for such checks to be triggered. A single failure by the operator to comply with the procedure, such as incorrectly filling up the QC form, could lead to the QC checks being bypassed.

12 Given that the first three statements of the print cycle would always be placed in a single envelope by the machine, there was a significant risk of every first envelope containing the statements of two or more individuals.

2 [2017] PDP Digest 81.

3 [2017] PDP Digest 107.

This, in turn, created a risk of the individual's statement being disclosed to another individual. The design and operation of the enveloping machine ensured that this risk arose with each print cycle. In the Commission's view, such risks could be avoided, for example, simply by having Sheet 1 print out blank pages by default, instead of statements containing information of actual customers. That way, the two other statements (of the three statements) in the first envelope would be blank statements, and there would be a lower chance of an unauthorised disclosure of a statement to the wrong recipient.

13 It was because of such risks that there needed to be a proper way of checking and ensuring that any additional statements were removed from the envelope. This again was where DPL failed: DPL relied entirely on a single operator for the correction to be made, and it did not have a proper system of checks and supervision over the operator's actions.

14 First, DPL's system of QC checks was inadequate. The operator was able to bypass both the second or third level checks, since the persons carrying out these checks were only checking envelopes found in the reject bin. The operator was able to remove the envelope from the reject bin and place it in the main bin. This resulted in there being no second or third level checks being carried out on the envelope in this case.

15 Second, there was no independent verification of the accuracy of the QC form filled in by the operator, which meant that the second and third level checkers would not have been aware of the fact that the operator had incorrectly moved an envelope from the reject bin to the main bin, as the numbers in the QC form appeared to tally with the expected total from the run. The second and third level checkers were essentially relying on the numbers provided by the operator in the QC form in order to ascertain whether an error or failure had occurred. Since there was no independent verification, the second and third level checkers could not ascertain if those numbers provided by the operator were actually correct. Accordingly, depending on how the QC form was filled up, the second and third level checks could easily be bypassed just by the QC form showing, on the face of it, that the numbers in the reject bin and main bin had tallied with the expected total from the run. The lack of an independent verification of the QC form, and the manner in which the second and third level checkers could be circumvented from the incorrect filling up of the QC form, was a

systemic weakness in DPL's QC process, and a failure to put in place adequate security arrangements to protect personal data.

16 Given the sensitivity of the personal data involved (financial statements), it was incumbent on DPL to ensure that its QC measures could not be so easily bypassed. The data breach could have been avoided if DPL had taken some simple additional precautions, for example:

(a) the second and third level checkers could have been obliged to check the digital counter, to ensure that the QC form filled in by the operator was accurate; and

(b) the operator could have been obliged to always return the first envelope filled by the machine to the reject bin which will ensure that it will be inspected by the second and third level checkers.

17 For the reasons above, the Commission finds that DPL had not put in adequate security arrangements to protect personal data. Accordingly, the Commission finds DPL in breach of s 24 of the PDPA.

## ENFORCEMENT ACTION BY PERSONAL DATA PROTECTION COMMISSION

18 Given that DPL breached its obligation under s 24 of the PDPA, the Commission is empowered under s 29(1) of the PDPA to issue such directions as it thinks fit in the circumstances.

19 The Commission finds that the personal data disclosed, being financial information, were sensitive in nature. This is a significant aggravating factor, warranting a financial penalty as a matter of general deterrence.

20 However, the Commission also notes the following mitigating factors:

(a) The scale of the breach was small. Only personal data belonging to two individuals were disclosed to a single recipient.

(b) There was no evidence to suggest that the data breach caused actual loss or damage to any person.

21 The Commission has therefore decided to impose a financial penalty of $3,000 on DPL.

22 In addition, the Commission also directs DPL to:

(a) conduct a review of its internal working procedure relating to data printing and enveloping operations, in particular to tighten the application of quality control checks;

(b) improve the training of all operators and quality checkers involved in its printing and enveloping operations; and

(c) review its personal data protection policy to determine if it needs to be updated to suit its current operations.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re Management Corporation Strata Title Plan No 3696 and another

## [2018] PDP Digest 215

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1610-B0275
**Decision Citation**: [2018] PDP Digest 215; [2017] SGPDPC 11

***Data intermediary*** *– Obligations of organisation and data intermediary*
***Protection Obligation*** *– Access to personal data – Insufficient physical and administrative security arrangements*

29 June 2017

### INTRODUCTION

1 Sometime in December 2015, the Personal Data Protection Commission ("Commission") had investigated into a complaint in relation to the failure by a security company to safeguard the visitor logbook of Prive Executive Condominium ("Condominium"), which contained personal data of the visitors. The security company was found in breach of s 24 of the Personal Data Protection Act 2012[1] ("PDPA") for leaving the logbook unattended and failing to protect the logbook from prying eyes. The case is published as *Re Spear Security Force Pte Ltd*.[2]

2 A similar breach has again taken place at this Condominium. This time round, the breach took place under another security company, the second respondent ("Eagle Eye"), which was engaged by the first respondent ("MCST 3696"), the Management Corporation Strata Title ("MCST") of the Condominium, for its security services.

1 Act 26 of 2012.
2 [2017] PDP Digest 87.

3 Following a complaint made to the Commission, the Commission proceeded to investigate into the matter. The Commission found both the first and second respondents in breach of their respective obligations under s 24 of the PDPA. The Commission now sets out its grounds of decision of the matter.

## MATERIAL FACTS

4 The data breach incident took place in the evening of 16 October 2016. The complainant ("Complainant") had observed that a logbook that was placed on a table next to the gantry into the Condominium was left unattended. The Complainant subsequently took photographs to show that the logbook was left open on the table and unattended by the security guards. These photographs were sent to the Commission for its investigation.

5 The gantry was about 30–50m away from the guardhouse, and led directly to the swimming pool of the Condominium. The logbook was used to record the attendance and details of the coaches who conduct swimming lessons at the Condominium. The logbook would therefore contain the dates and times of entry into the Condominium and the NRIC numbers of the coaches.

6 Based on the Commission's investigation, the Commission found that there was no security guard attending to the logbook from the hours of 8.00pm to 10.30pm. There was supposed to be a night-shift security guard to be stationed at the table where the logbook was located. However, the night-shift guard had reported that he was ill that evening, and his replacement had only arrived for duty at 10.30pm. Accordingly, the only security guards that were in the vicinity from 8.00pm to 10.30pm were the security guards that were stationed at the guardhouse, away from the gantry.

7 Although the security guards were stationed at the guardhouse, Eagle Eye claimed that they were within close proximity of the logbook, and keeping an eye whilst in the guardhouse.

8 MCST 3696 and Eagle Eye also claimed that the security guards had previously been specifically instructed to close the logbook when not in use and to keep the book in the guardhouse if no security guard was stationed at the table. Additionally, they claimed that these security guards were

reminded to exercise due care and diligence to safeguard personal data, advised on the PDPA and warned about the severity of the penalty for disclosure of personal data.

9 Following the data breach incident, MCST 3696 and Eagle Eye had removed the table at the Condominium gantry so that all visitor registrations would only be done at the guardhouse. This was to ensure that the logbook was kept in the guardhouse at all times.

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS

10 The information that was contained in the logbook, namely, the NRIC number and the dates and times of the entry and departure from the Condominium, would constitute "personal data" under s 2 of the PDPA of the coaches who came to the Condominium. The information allows for the identification of the individual, and the date and timings at which the individual had entered and left the premises. In particular, the NRIC numbers of the coaches are generally considered to be of a sensitive nature, as it is widely used for business purposes and transactions with the Government,[3] and could be used to cause harm should such information fall into the wrong hands.

11 Accordingly, since the logbook contains personal data of the individual coaches, it must be protected under s 24 of the PDPA.

12 The issues that arise from this case are as follow:

(a) what the relationship between MCST 3696 and Eagle Eye was, and what their respective obligations under the PDPA were; and

(b) whether MCST 3696 and Eagle Eye complied with their respective obligations under the PDPA.

### *Relationship between MCST 3696 and Eagle Eye and their respective obligations*

13 MCST 3696 had engaged Eagle Eye to provide security guard services pursuant to an agreement on 15 August 2016.

---

3 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics – NRIC Numbers*.

14 As part of the security services, Eagle Eye was to record the movement of persons entering or leaving the premises of the Condominium. This included maintaining a logbook of coaches who were entering or leaving the premises of the Condominium.

15 The recording and safekeeping of the logbook were activities that fall under the definition of "processing" of personal data under s 2(1) of the PDPA. Given that MCST 3696 had engaged Eagle Eye to carry out such services (as part of the overall security services), Eagle Eye was a data intermediary to MCST 3696 (the organisation) in relation to the handling and safekeeping of the logbook.

16 As an organisation, MCST 3696 has the primary role and duty to protect personal data in its possession or control under s 24 of the PDPA. The organisation held the primary role and duty to protect personal data, even though it had engaged a data intermediary to protect the personal data as well. This principle has been elucidated in the case of *Re The Cellar Door Pte Ltd*.[4] As for Eagle Eye, although it has fewer obligations to meet under the PDPA (pursuant to s 4(2) of the PDPA), it still needs to protect personal data in its possession under s 24 of the PDPA.

17 We now turn to examine whether MCST 3696 and Eagle Eye have complied with their respective obligations to protect the logbook under s 24 of the PDPA.

### *Whether MCST 3696 and Eagle Eye have complied with their respective obligations to protect personal data under section 24 of the Personal Data Protection Act*

18 In relation to Eagle Eye, the Commission has found Eagle Eye to be in breach of its obligations under s 24 of the PDPA.

19 First, whilst Eagle Eye claims that it had informed the security guard to keep the logbook closed when not in use and to keep the book in the guardhouse if no security guard was stationed at the table, the instructions were clearly ineffective, as none of the security guards had carried out those instructions. As the Complainant had found on 16 October 2016, the logbook was left unattended and open on the table. Further, the instructions themselves were bare and incomplete, as they do not, for

4 [2017] PDP Digest 160.

example, inform the security guards how to organise themselves to ensure that the logbook is closed at all times when not in use, or who was responsible to carry out the task. The failure by Eagle Eye to provide proper instructions to its security guards was a dereliction of its duty to ensure that there were reasonable security arrangements to protect the personal data in the logbook.

20 Moreover, it was not enough for the organisation to simply provide instructions to the security guards to safekeep the logbook without doing more – *ie*, putting in place actual processes or practices to protect the logbook. Without having actual processes or practices in place to protect personal data, Eagle Eye's instructions were but empty instructions with little effect. This can be seen in the manner in which the security of the logbook appears to have been carried out: on an *ad hoc* basis, where there was no co-ordinated and comprehensive effort to ensure that the logbook was safeguarded or safekept with the security guards at all times. And indeed, this has been laid bare by the Complainant being able to take photographs of the logbook without the security guards noticing.

21 Additionally, the alleged instructions were not documented. This makes it hard to disseminate the message to all the security guards, especially to the new employees joining the organisation. As discussed in *Re Furnituremart.sg*,[5] without having written policies or practices, it would be difficult to promulgate the policies or practices effectively to the employees and staff of the organisation.

22 Second, while Eagle Eye had a data protection policy in place, the policy was spartan in terms of the policies that govern the protection of the logbook. The only reference to the protection of personal data was a line which mentioned:

> To ensure that personal rights to confidentiality are respected in compliance with the Personal Data Protection Act 2012 and no disclosure of personal data of resident, visitor, contractor, vendor, delivery and *etc*.

The policy does not elaborate further on how these may be translated into actual practices or processes to protect the logbook. As mentioned in *Re Tiger Airways Singapore Pte Ltd*,[6] it is important for an organisation to

5 [2018] PDP Digest 175.

6 [2018] PDP Digest 166.

ensure that its policies are contextualised to its operations, so that they are pertinent and relevant to the organisation's work or operations on the ground, and meaningful and useful to employees in the context of their work or responsibilities. A simple or bare statement in a policy telling employees to comply with the PDPA (for example) would not actually inform them how to protect personal data in the context of what they are doing.

23 Third, Eagle Eye did not seem to have a contingency plan for the safekeeping of the logbook when the security guard fell sick and had to be replaced by another security guard. When the replacement guard came late, that had apparently led to the shortage of a security guard to be stationed at the table to look after the logbook. Rather than returning the logbook to the guardhouse, the logbook was simply left on the table unattended. In the Commission's view, there ought to have been some form of system or process to ensure that when the security guards are unavailable to be stationed at the table, the logbook would, by default, be returned back to the guardhouse for safekeeping. Again, this accentuates the point that there was no system in place to ensure the proper safekeeping of the logbook.

24 Eagle Eye claimed that its security guards were in close proximity of the logbook, since they were stationed at the guardhouse, and had kept an eye on the logbook. However, this was not the same as safeguarding the logbook itself. The fact that the Complainant was easily able to take photographs of the contents of the logbook and the surroundings, without any of the security guards noticing, is testament to the need for having close supervision of the logbook, which may only be achieved in this case by keeping the logbook with the security guards. By being stationed at the guardhouse, this made supervision and monitoring of the logbook difficult, and increased the risk of the security guards being blind-sided to any unauthorised access to the logbook that was left at the table. The difficulty of supervision and monitoring was exacerbated by the fact that the security guards' attention would have been diverted (at times) to the activities at the guardhouse, and away from the logbook.

25 With regards to MCST 3696, it had the primary and shared responsibility with Eagle Eye to protect personal data.

26 The need to meet this primary responsibility ought to have been drawn into sharp focus for MCST 3696, as this was not the first time that the hired security guards of the Condominium had left the logbook

unattended. As mentioned above, the Commission had found the previous security guard company to be in breach of the PDPA for a similar incident, and had been issued a warning for it. Given that the previous security company was issued such a warning, MCST 3696 ought to have exercised closer supervision over the implementation and adoption of the policies and practices to protect the personal data collected by the Condominium. For example, by engaging with Eagle Eye in the planning and development of policies and practices that would be appropriate in the Condominium's setting to protect personal data, or by having general oversight over the security of the personal data. After all, having gone through the previous experience of the data breach incident, there would have been lessons learnt and improvements to be made, which MCST 3696 could have imparted or shared with the incoming security guard company, Eagle Eye, for developing its policies and practices to protect personal data at the Condominium.

27 However, MCST 3696 had failed to meet this primary responsibility to protect personal data. As mentioned above, the Commission has found a lack of adequate policies and processes that were in place to protect personal data. This is evident, given there was only one line in Eagle Eye's policy on personal data protection. Next, it was already established above that there was no system in place at the Condominium for the safekeeping of the logbook at all times – and indeed, the logbook was found to be left open on the table in this case. Additionally, from the responses provided to the Commission, it would appear that the only thing that MCST 3696 did was to remind the security guards at the meeting to secure the logbook, which fell far short of providing that supervision and oversight (described above) for the protection of personal data.

28 Given MCST 3696's failure to provide that supervision and oversight to ensure the security of the personal data in the logbook, the Commission has found MCST 3696 to also be in breach of s 24 of the PDPA.

## ACTIONS TAKEN BY PERSONAL DATA PROTECTION COMMISSION

29 For the reasons above, the Commission has found that both Eagle Eye and MCST 3696 are in breach of their respective obligations under s 24 of the PDPA. In this regard the Commission is empowered under s 29 of the PDPA to give Eagle Eye and MCST 3696 such directions as it deems fit to

ensure compliance with the PDPA. This may include directing the respondent to pay a financial penalty of such amount not exceeding $1m as the Commission thinks fit.

30 However, in view that Eagle Eye and MCST 3696 have taken reasonably adequate steps to remedy the lapses, as set out above at [10], during the course of the investigations, the Commission has decided not to impose any directions against them. Instead, it has decided to issue a Warning against Eagle Eye and MCST 3696 for the breach of their respective obligations under s 24 of the PDPA.

31 The Commission emphasises that it takes a very serious view of any instance of non-compliance with the PDPA, and it urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re Orchard Turn Developments Pte Ltd

## [2018] PDP Digest 223

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-1512-A612
**Decision Citation**: [2018] PDP Digest 223; [2017] SGPDPC 12

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

6 July 2017

## BACKGROUND

1 In this case, the complainant received two unauthorised e-mails, purportedly sent by the organisation ("Organisation") promoting "free" ION+ Reward points. Investigations discovered that an unknown perpetrator had gained unauthorised access to a server that held personal data of the Organisation's members. The perpetrator then used an application on the compromised server to send the unauthorised e-mails to the Organisation's members using their personal data that were held in the server. This data breach incident raised the question of whether the Organisation had met its protection obligation under the Personal Data Protection Act 2012[1] ("PDPA") to make reasonable security arrangements to sufficiently protect personal data held on the server.

2 The following sets out the Personal Data Protection Commission's ("Commission") findings following its investigations into the matter.

1 Act 26 of 2012.

## MATERIAL FACTS AND DOCUMENTS

3 The Organisation is the property manager of ION Orchard, a retail mall in Singapore. The Organisation runs the ION+ Rewards Loyalty Programme ("ION's Loyalty Programme"), which awards its members points based on their purchases made at the mall. Super e-Management Limited ("Super-E"), a Hong Kong-based information technology ("IT") service provider, manages the IT system for ION's Loyalty Programme.

### *System setup*

4 ION's Loyalty Programme runs on the Loyalty Management System ("LMS") which comprises several interconnected servers. Only two servers are relevant to the Commission's investigation: the (a) web and electronic direct mailer server ("EDM server") and (b) LMS and reporting server ("LMS server"). The LMS server was used to store the database of members' personal data, while the EDM server was used to send out e-mails to members of ION's Loyalty Programme who had subscribed to receive updates from ION Orchard.

5 For the purpose of sending these e-mail updates to its subscribers, the Organisation would transfer a subscriber list containing personal data of the Organisation's subscribers on the LMS server to the EDM server every day. This transfer of the subscriber list from the LMS server to the EDM server was an automated process. The Organisation would then send these e-mails through a web application hosted on the EDM server ("EDM Application"), which was configured to allow access to users with an administrative account ("admin account"). After the Organisation had sent out the e-mails, the personal data of the subscribers were not purged but were instead retained on the EDM server. The personal data set that was stored on the EDM server comprised a subscriber's name, e-mail address, birthdate and membership registration date.

### *Data breach incident*

6 On 26 December 2015, an unknown perpetrator gained unauthorised access to the EDM Application using valid admin account credentials to access the subscriber list. The perpetrator then crafted unauthorised e-mails, which looked like they were genuine e-mails from the Organisation, promoting "free" ION+ Reward points ("Phishing E-mails") to the

subscribers; before proceeding to send these Phishing E-mails out to 24,913 subscribers.

7 The Phishing E-mails contained a link (<http://fastlnks.com/7LIW>) which directed a subscriber to an online advertisement website. The subscriber would be prompted to select one of the options on the website to obtain the bogus ION+ Reward points. If the subscriber selected any of the options, the subscriber would be directed to more advertisement pages which might request for the subscriber's personal data, such as the subscriber's mobile phone number or e-mail address.

8 Subsequently, Super-E received an alert from the EDM server and discovered that an Internet Protocol address ("IP address") from Egypt had successfully logged into the system, and had sent out the Phishing E-mails to the Organisation's subscribers. After discovery of the data breach, Super-E disabled the EDM server to prevent further dispatches of Phishing E-mails to the Organisation's subscribers. On 27 and 29 December 2015, the Organisation sent e-mails to the affected subscribers informing them of the Phishing E-mails that had been sent.

### *KPMG reports*

9 The Organisation engaged KPMG Services Pte Ltd ("KPMG") to conduct an investigation into the data breach incident. KPMG found that the cause of the incident appeared to be "an unauthorised access using 'admin' credentials via the EDM application".

10 In addition, KPMG found several issues with the security posture of the EDM server. For example, KPMG found that the operating system of the EDM server was not patched or hardened, thus exposing the EDM server to potential exploitation. Additionally, KPMG conducted a vulnerability check which revealed that the EDM Application had 24 known vulnerabilities that could be exploited.

### *Personal Data Protection Commission's investigations into Super-E*

11 Based on the Commission's investigations into the matter, the Commission understands that Super-E was involved in the management of the IT systems for the ION Loyalty Programme at the time of the data breach incident, and may therefore share some responsibility with ION for

the protection of the personal data of the Organisation's subscribers. As Super-E is located in the Hong Kong Special Administrative Region of the People's Republic of China, the Commission would pursue available options for assistance in this aspect of the investigations with the relevant foreign data protection authority.

12 In the meantime, the Commission has concluded its investigations into the Organisation's compliance with the PDPA, and has therefore proceeded to issue its grounds of decision focusing only on the Organisation's compliance with the PDPA.

## PERSONAL DATA PROTECTION COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

### *Issues for determination*

13 The relevant issue for determination is whether the Organisation had put in place reasonable security arrangements to protect the personal data set in its possession or in its control, as required under s 24 of the PDPA.

### *Whether the Organisation was in breach of section 24 of the Personal Data Protection Act*

#### *Increased risk due to the Organisation's system setup*

14 As described above at [4]–[5], the Organisation did not purge the personal data from the EDM server that were being transferred every day from the LMS server to the EDM server. After the e-mails had been sent out, the personal data of the subscribers were not deleted from the EDM server. The effect of this practice was that some of the personal data of the Organisation's members could be found in two different places – the LMS server and EDM server.

15 However, this retention of personal data on the EDM server was unnecessary. The LMS setup was designed in such a way that the primary database of customer data was stored on the LMS server, which had no direct connection to the Internet. The EDM server, on the other hand, was a separate server that had access to the Internet. Given that a subset of members' personal data was automatically transferred from the LMS server

to the EDM server every day, only this subset of personal data was accessible from the Internet. Once the subscribers' personal data had been transferred to the EDM server, the process for each e-mail blast was as follows: load the subset of personal data of subscribers, run the EDM Application, and use the EDM Application to blast the e-mails to the subscribers. There was no need to retain the personal data in the EDM server beyond this. The daily automatic transfer of data from the LMS server to the EDM server coupled with the retention of personal data on the EDM server created significant risks to the security of the personal data.

16 First, the daily automatic transfer effectively created a permanent store of personal data on the EDM server. This *de facto* permanent store of personal data had the effect of storing a duplicate or additional set of personal data on the EDM server (in addition to the LMS server). The EDM server was accessible from the Internet and its online accessibility made it more susceptible to online attacks and external threats, and it was therefore more likely to be compromised. By keeping a duplicate or additional set of personal data on the EDM server, the Organisation was placing unnecessary risks on the security of the personal data, should the EDM server be the subject of an attack or security compromise.

17 Second, the longer the personal data set was left on the EDM server, the more exposed it was to online attacks and external threats. If personal data is loaded onto the EDM server whenever there is – and only for the duration of – a scheduled e-mail blast, and then promptly deleted, there would not have been a *de facto* permanent store of personal data on the EDM server. Prompt deletion after each e-mail blast would significantly narrow the window period for which the personal data on the EDM server are at risk of unauthorised access in the event that the EDM server is compromised. During investigations, the Commission discovered that the e-mail blast is scheduled to take place approximately once a month. Further, in any given month, another e-mail blast would also be made on an *ad hoc* basis to certain categories of ION members (a subset of all subscribers). The aforesaid e-mail blast would, therefore, be likely sent out via the EDM server more than once a month. It cannot be gainsaid that the risk had been significantly enlarged by keeping a *de facto* permanent store of personal data on the EDM server.

18 Third, the frequency of such transfers brings about an increased risk that personal data may be intercepted during transmission. In this regard,

the daily automatic transfer of personal data from the LMS server to the EDM server, when compared with the much less frequent e-mail blasts to subscribers (approximately on a monthly basis), exposes the personal data *in transit* to an unnecessarily enlarged risk of interception.

19 Additionally, by effectively establishing a permanent store of personal data on the EDM server (albeit a subset of subscribers who wished to received EDM e-mails), and given the attendant risks attached to it, there was a need for the Organisation to ensure that the extent of hardening the EDM server and security of the transmission route to the EDM server can meet the level of protection expected in order to comply with the PDPA. Once a server is known to hold or process personal data, the organisation has obligations to protect the personal data by ensuring that the personal data in transit to and from the server, and the personal data held in the server, are adequately protected.

20 In the final analysis, it was not prudent for the Organisation to keep a duplicate or additional set of personal data on the EDM server for a period longer than necessary. Accordingly, the Organisation's setup of the LMS in combination with its practice of retaining the personal data set on the EDM server was not in keeping with the reasonable security arrangements to be put in place.

21 In addressing the issues highlighted above, the Organisation may seek to include the standards for compliance with the protection obligation as part of its design specifications of the LMS. By adopting a data protection-by-design approach towards the enhancements to the LMS, it is conceivable that no more than modest enhancements may be necessary in order to meet the standards expected for compliance with the PDPA.

*Absence of proper policies or practices to safeguard passwords*

22 The Commission also identified other issues concerning the security of the members' personal data. Foremost of them is the absence of policies or practices to safeguard the admin account passwords.

23 Although the Organisation was unable to establish the root cause of the data breach incident, what the Organisation, KPMG and Super-E had found was that the perpetrator had gained unauthorised access to the EDM server in a single attempt. There was no evidence of hacking or that the perpetrator had deployed any brute force attacks. This suggests that it was

likely that the perpetrator had managed to get hold of the valid admin account credentials to gain access to the EDM system.

24 In the course of investigations, the issue of whether the Organisation had put in place proper password management practices and policies came to the fore. The Commission found that the Organisation did not have any formal policy or practice for the management of the admin account passwords to the EDM server. In particular, the Organisation failed to implement any policy to prohibit the sharing of admin account credentials or to enforce periodic expiry and renewal of the same. In the following sections, we will look at the various authorities highlighting the importance of having proper password management policies and practices, and examine the organisation's failure to put in place proper password management policies and practices in this respect.

### (i) Foreign authorities highlight importance of password management policies

25 The need for proper password management policies was highlighted in the report *Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*[2] ("Joint Investigation"). In that case, Avid Life Media Inc ("ALM"), a company incorporated in Canada that operates a number of dating websites including Ashley Madison, was the subject of a data breach incident in 2015. The hackers gained access to the details of 36 million ALM user accounts, which included personal information, and published the data online.

26 In their joint report, the commissioners found that ALM had poor key and password management practices, given that it had made available on ALM's Google drive, the "shared secret" to its Virtual Private Network ("VPN"). This meant that "anyone with access to any ALM employee's drive on any computer, anywhere, could have potentially discovered the shared secret". The commissioners concluded that such practices

2 *PIPEDA Report of Findings #2016-005: Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/ Acting Australian Information Commissioner* (22 August 2016) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/>.

constituted "failures to take reasonable steps to implement appropriate security safeguards in the specific circumstances, given the volume and nature of the personal information held by ALM".

27 That the need for proper password management policies forms an important component of the security arrangements to protect personal data is also found in the case of *Twitter, Inc*.[3]

28 In that case, the Federal Trade Commission ("FTC") found that Twitter, a social networking website, had failed to, amongst other things, enforce periodic changes of admin account passwords, *eg*, by setting passwords to expire every 90 days. Additionally, Twitter also failed to establish or enforce policies sufficient to make admin account passwords hard to guess. Accordingly, Twitter was found to have failed to provide reasonable and appropriate security measures to protect personal data.

(ii) Foreign authorities highlight importance of regular changing of passwords and prohibition against sharing of credentials

29 Data protection authorities are also of the view that good password management policies encompass the regular changing of admin account passwords and the prohibition against sharing admin account credentials amongst multiple users.

30 The abovementioned case of *Twitter, Inc* also stands for the point that there needs to be periodic changes to the admin account passwords. The effect of implementing periodic changes is that there will be a shorter window period, and thus fewer opportunities, for someone to try to crack the admin account passwords of the system.

31 Additionally, there should not be a sharing of credentials amongst users. When credentials are shared among multiple users, it is difficult to ensure accountability as it is difficult to track the activity of each individual using the common set of credentials.

---

3 *In the Matter of Twitter, Inc* (2 March 2011), FTC 092-3093 (No C-4316) <https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation>.

32 In the case of *Reed Elsevier Inc and Seisint, Inc*,[4] the organisations had collected and stored in their databases non-public and highly sensitive personal information about millions of consumers, including consumer identification information obtained from credit reporting agencies. Attackers exploited the organisations' poor security practices to obtain the user credentials of legitimate consumers, and used these credentials to make thousands of unauthorised searches for consumer information in the organisations' databases. The FTC found that the organisations had failed to adequately protect personal data because they had, amongst other things, a practice of permitting the sharing of user credentials among a customer's multiple users. According to the FTC, this had the effect of reducing the likely detection of, and accountability for, unauthorised access to the databases.

33 In this regard, the Information Commissioner's Office ("ICO") in the UK has advised organisations to "issue all staff with unique usernames and passwords for the network and systems containing personal data", and "do not allow users to share passwords with their colleagues".[5] Likewise, the Office of the Data Protection Commissioner of Ireland has expressly stated in its *Data Security Guidance* that "[s]hared credentials should never be permitted" and that data controllers should "ensure that users are made aware that their password/passphrase is unique to them and must not be disclosed to anyone else".[6]

34 In sum, the data protection authorities have taken the position that password management policies, especially the regular changing of passwords and prohibition against the sharing of credentials, are an important and integral part of IT security arrangements.

---

4 *In the Matter of Reed Elsevier Inc and Seisint, Inc* (1 August 2008), FTC 0523094 (No C-4226) <https://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter>.

5 UK, Information Commissioner's Office, *Findings from ICO Advisory Visits to Residential Sales and Lettings Organisations* (2016) <https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/1560562/outcomes-report-residential-sales-and-lettings.pdf> at p 7.

6 Republic of Ireland, Office of the Data Protection Commissioner of Ireland, *Data Security Guidance* <https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm>.

(iii) Organisation failed to implement proper password management policies required

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:

> (a) first, the Organisation only created a single admin account, of which the admin account credentials were shared among four authorised users. All these four users were sent the same admin account credentials in a single e-mail from Super-E dated 28 January 2015. This "sharing" of the admin account credentials multiplied the risks of a data breach by making it more difficult to pinpoint which user had been the source of the likely leak of credentials that enabled the unauthorised access to take place. At the same time, the EDM server would not have been able to ascertain (and account for) which of the users (whether authorised or not) had accessed the system, since the username and password was the same for all; and
>
> (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, *ie*, 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.

36 Accordingly, given the lack of proper password management policies and practices, the Commission was of the view that the Organisation had failed to put in place reasonable security arrangements to protect the members' personal data.

*Other issues with the Organisation's security arrangements*

37 Apart from the issues with the password management policies of the EDM server, the Commission also found other notable issues as follows.

38 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.

39 Second, the Organisation did not conduct any vulnerability assessment to detect if there were any vulnerabilities in the system prior to its roll out. As explained in *Re The Cellar Door Pte Ltd*,[7] this meant that there was no systematic way of identifying vulnerabilities, and addressing those vulnerabilities. This posed as a limitation to the Organisation's ability to determine the technical measures that were required to ensure that the personal data of its members were adequately protected.

40 The Commission understands that after the data breach incident, the Organisation purged all the personal data residing on the EDM server and subsequently put in place a purge policy where the personal data set on the EDM server will be removed after a standard period of 14 days.

41 In view of all of the relevant facts and circumstances, the Commission finds that the Organisation has not made reasonable security arrangements to protect personal data and is in breach of s 24 of the PDPA.

## PERSONAL DATA PROTECTION COMMISSION'S DIRECTIONS

42 Given that the Commission has found the Organisation to be in breach of s 24 of the PDPA, the Commission 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 $1m as the Commission thinks fit.

43 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commission took into account the following factors:

7 [2017] PDP Digest 160.

(a) a large number of individuals (a total of 24,913 subscribers out of a potential 47,635 subscribers that could have been impacted by the data breach incident) had the unauthorised Phishing E-mails sent to them;

(b) the Phishing E-mails had exposed the recipients to further risks and other exploits, *ie*, through the pop-up windows that were intended to induce the recipients to provide their personal data;

(c) the Organisation did not make reasonable efforts to put in place proper password management policies, and to ensure the security of the personal data set by reasonably anticipating, identifying and rectifying the technical security vulnerabilities (as mentioned at [38] and [39] above) at an earlier stage;

(d) the Organisation was generally co-operative and forthcoming in providing timely responses to the Commission during the investigation; and

(e) the Organisation took prompt remedial action after being alerted to the data breach incident, as well as other corrective measures to improve its IT security.

44 Having carefully considered all the relevant factors of this case, the Commission hereby directs the Organisation to do the following:

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

(i) patch all the system vulnerabilities identified by the KPMG reports dated 8 March 2016 and 19 April 2016;

(ii) conduct a penetration test on the Internet-facing portion of the Loyalty Management System and rectify weaknesses that have been identified; and

(iii) implement a password management policy and conduct training for staff on password management best practices;

(b) by no later than 14 days after the above action at [44(a)] has been carried out, the Organisation shall, in addition, submit to the Commission a written update providing details on (i) the results of the penetration test; (ii) the measures that were taken by the Organisation to patch all system vulnerabilities; and (iii) the password management policy and the training; and

(c) pay a financial penalty of $15,000 within 30 days from the date of the Commission's direction, failing which, interest at the rate of 6% per annum 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**
**Personal Data Protection Commission**

Grounds of Decision

## Re Ang Rui Song

## [2018] PDP Digest 236

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-1610-B0257
**Decision Citation**: [2018] PDP Digest 236; [2017] SGPDPC 13

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

14 August 2017

### BACKGROUND

1 This is a case of a financial consultant (an "organisation" under the Personal Data Protection Act 2012[1] ("PDPA")) ("Respondent" or "Organisation") who improperly disposed of his clients' insurance policy related documents, which contained sensitive personal data ("Prudential folders"). The documents were discovered by the complainant ("Complainant") at a rubbish bin of a residential estate.

2 Following an investigation into the matter, the Commissioner found that the Respondent is in breach of s 24 of the PDPA. The Commissioner's findings of this matter are set out below.

### MATERIAL FACTS AND DOCUMENTS

3 The Respondent was a financial consultant with Prudential Assurance Company (Pte) Ltd ("Prudential"). The terms of his engagement as a financial consultant was such that the Respondent was an independent contractor and not an employee of Prudential. During his engagement as a financial consultant, the Respondent came into possession of his clients'

1 Act 26 of 2012.

Prudential folders. However, at the time that the Respondent disposed of these documents, he was no longer with Prudential.

4 On 10 October 2016, the Commissioner was informed by the Complainant that the Prudential folders had been disposed of by leaving beside the rubbish bin at level two of the multi-storey car park at Block 821A Jurong West Street 81. Upon further inspection, the Complainant found that the Prudential folders contained 13 certificates of life assurance issued by Prudential, and bore the names of 12 individuals, in addition to two letters addressed to two of the aforementioned individuals.

5 The folders contained information on 12 of Prudential's policyholders. Taken collectively, the information identified the individual policyholders, which included the following pieces of personal data:

(a) name of policy holder;
(b) NRIC number;
(c) benefits;
(d) sum assured;
(e) cover start date;
(f) cover expiry date; and
(g) premium.

The full list of information is set out in the Schedule of this grounds of decision.

6 The two letters were addressed to two of the 12 policyholders mentioned above, and contained the following personal data:

(a) name of policy owner;
(b) address;
(c) policy number; and
(d) name of life assured (same as the policy owner).

7 During investigations, the Respondent confirmed that he had disposed of the folders containing the abovementioned personal data at the location where they were found by the Complainant. The disposal was made under the instructions of the Complainant's clients. However, he claimed that he had disposed of them in the bin, and not by leaving them beside the rubbish bin. The Complainant also claimed that he had placed the documents in a plastic bag before disposal.

## COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

### *Respondent's obligation to protect personal data under section 24 of the Personal Data Protection Act*

8 As a preliminary issue, the Commissioner had considered the following question: was the Respondent acting as an "organisation" for the purposes of the PDPA in respect of the personal data contained in the Prudential folders? If so, then, as an "organisation", he has an obligation to protect the personal data under s 24 of the PDPA.

9 The definition of "organisation" under the PDPA expressly includes "any individual" and would apply to an individual such as the Respondent.

10 At the time the Respondent joined Prudential, he was, according to his contract, acting as an independent contractor of Prudential, and not as an employee. In dealing with his clients' personal data, he had control and autonomy over the management of the personal data. For example, he had control over how the policy folders were stored and kept in his care, and the provision and receipt of the policy documents from his clients. Accordingly, the Respondent was an "organisation" under the PDPA, and had an obligation under s 24 of the PDPA to protect the personal data he had collected.

11 This obligation stayed with the Respondent (as an "organisation") throughout the time that he was with Prudential, and even after he had left his engagement with Prudential. This is in line with the principles in *Re Chua Yong Boon Justin*,[2] where the respondent was a registered salesperson who obtained personal data of the complainant and his wife in the course of his real estate agency work and hence in the course of carrying on his business. Having obtained such personal data in a capacity that is not "personal or domestic", the Personal Data Protection Commission held that the respondent was not allowed to claim that the subsequent disclosure of the personal data was made in a "personal or domestic capacity", which would have allowed him to dispense with the need to obtain consent under s 4(1)(*a*) of the PDPA. In *Re Chua Yong Boon Justin*, the Personal Data Protection Commission held that the respondent continued to hold such

2 [2017] PDP Digest 91.

personal data in the course of his business, and needed to comply with his consent obligation when disclosing the personal data. Similarly, in the present case, the Respondent had obtained the personal data during the course of his work as a financial consultant and an "organisation" under the PDPA – *viz* not in a personal or domestic capacity. He therefore had a duty to protect the personal data throughout – whilst with Prudential and after he left Prudential. The Respondent cannot unilaterally change the capacity in which he possesses the personal data, even after he ceased being a financial consultant with Prudential. The Respondent remained obliged to comply with s 24 of the PDPA at all material times.

12 In respect of the role of Prudential, the Commissioner found Prudential not to be responsible (or liable) for the proper disposal of the policy documents, or the data breach incident that has occurred. Prudential had reasonable policies in place which dealt with proper and secure disposal of clients' policy documents. The pertinent policies required financial advisers to return client data to Prudential when they ceased being financial advisers, or (alternatively) to dispose of personal data properly and securely – for example, by shredding. Prudential had communicated these policies through appropriate channels. Indeed, in accepting the Respondent's resignation, Prudential had issued a letter specifically referring to the need to "return all monies, documents and other effects and property belonging to [Prudential] including such property containing customer information".

13 In the Commissioner's view, therefore, it was the Respondent who had full responsibility in the protection and proper disposal of the personal data found in the Prudential folders. We now turn to the analysis of whether the Respondent has complied with this obligation.

### *Whether Respondent's manner of disposal of Prudential folders was a breach of section 24 of the Personal Data Protection Act*

14 When it comes to the disposal of documents containing personal data, there is a need to ensure that the disposal is carried out properly and in a secure manner in order to meet the requirements of s 24. Section 24 requires an organisation to "make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". In this case, a reasonable security

arrangement meant proper and secure disposal of the Prudential folders, which would prevent any of the risks mentioned.

15 The PDPC's *Guide to Disposal of Personal Data on Physical Medium* ("PDPC's Guide to Disposal") sets out some useful principles undergirding the proper disposal of documents containing personal data in this regard. Some of these principles are relevant to the present case and are set out below. As mentioned in the PDPC's Guide to Disposal, in order to comply with s 24 of the PDPA, it may not be enough for an organisation to simply discard documents containing personal data in the physical trash bin. This may lead to an incomplete or improper disposal of personal data, which opens up to potential data breaches:

> (a) deleted electronic files or improperly shredded paper may be restored (in full or partially); and
>
> (b) uncontrolled disposal of paper without destruction may lead to recovery of documents through "dumpster diving" (*eg*, sifting through physical waste or recycling containers for items that have been discarded, but are still of value or covered by regulation).

16 Instead, for personal data stored on physical media and in paper form, the PDPC's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, advises organisations to ensure proper disposal of the documents that are no longer needed, through shredding or other appropriate means. This includes one or more of the following processes:

> (a) incineration (or burning): reduces paper to ashes;
>
> (b) shredding: cuts paper in a way that makes it reasonably difficult, or even impossible to reassemble the pieces in order to reconstruct (a substantial part of) the information, but allows for the paper to be recycled as long as the pieces are not too small; or
>
> (c) pulping: paper is mixed with water and chemicals to break down the paper fibres before it is processed into recycled paper.

17 The PDPC's Guide to Disposal also cautions that leaving documents containing personal data unattended while they await being discarded or destroyed may provide opportunities for a third party to gain access to the information, *eg*, leaving them at the rear entrance of the office, or at the bottom of the building, for collection by the paper disposal vendor. Generally, if the unauthorised disclosure of the information contained on the paper document could result in significant impact to an individual, organisations should consider shredding the document to cut the paper into

separate small pieces, which make it more difficult to reassemble. The more sensitive the information, the higher the level of shredding that needs to be done.

18 In this case, the Respondent's mode of disposal is wholly inadequate, especially given the type and sensitivity of the personal data found in the Prudential folders, and based on the circumstances. There are several reasons for the Commissioner's finding in this regard.

19 Based on the Respondent's representations, the documents were simply put in a plastic bag, tied up and placed inside the trash bin. The documents (and their contents) were left in their original readable form, and anyone could easily open the plastic bag to access the contents of the documents, especially the sensitive personal data of clients. It is foreseeable that random members of the public may dive into rubbish bins to retrieve disposed items that are recyclable, which is likely to include paper waste.

20 Additionally, with regards to the use of the plastic bag, this did not actually have the effect of securing the documents – just a mere concealment of the documents. While the mere concealment of documents may, in certain contexts, be enough when disposing of documents that contain little or no personal data of individuals, this was not appropriate in the present case.

21 The manner of disposal was inappropriate given the sensitivity of information found in the documents, such as the policy holder's name, NRIC number, premium amounts, name of life assured, benefits and sums assured, and maturity date. Based on what was pronounced earlier at [16]–[18] above, the sensitivity of such personal data warrants there to be a greater form of protection in the disposal of these documents. In the Commissioner's view, this can only be achieved by shredding the documents. As to the level of shredding, this should be guided by the level of sensitivity of the personal data contained in the document.[3] In the present case, the Respondent failed to carry out such shredding of the documents when disposing of these documents.

22 Additionally, Prudential had provided its agents and financial consultants designated "locked console boxes" for the secure shredding of

3 See Personal Data Protection Commission, *Guide to Disposal of Personal Data on Physical Medium* at paras 7.3–7.5.

unwanted documents. Prudential had informed its agents and financial consultants of this service and encouraged them to use it by way of a circular that was sent out on 12 January 2016.

23 The Respondent did not use this service for disposing of the policy documents at any point in time. Before leaving Prudential, Prudential had, as part of its standard practice, informed the Respondent to return the documents containing customer data to them, but the Respondent did not do so. When asked why he had not used the locked console boxes provided by Prudential, the Respondent mentioned that the locked console boxes were found in the main office of Prudential, and he was working at the branch office of Prudential. In other words, his excuse was that he seldom went over to the main office and thus it was inconvenient for him to make use of the locked console boxes. The Commissioner does not find this excuse to be acceptable, particularly since this could have been done as part of his end-of-contract administration.

24 Accordingly, the Respondent had available the means of securely disposing of the documents, *ie*, by way of the locked console boxes, shredding or similar means, but he chose not to use such methods of disposal. Instead, he had carried out the disposal in an unsecured manner described above. It would appear that his choice not to use the locked console boxes as provided by Prudential was borne out of convenience. The fact that Prudential had provided such means of disposing of the documents should have given the Respondent an indication that such documents ought to at least be securely disposed of by shredding. However, the Respondent did not adhere to such a standard of disposal of documents.

25 For the reasons above, the Commissioner finds that the Respondent failed to take reasonable security measures to protect the personal data in his possession and/or under his control and is in breach of s 24 of the PDPA.

## ENFORCEMENT ACTION BY COMMISSIONER

26 In exercise of the power conferred upon the Commissioner pursuant to s 29 of the PDPA, the Commissioner directs that a financial penalty of $1,000 be imposed on the Organisation.

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

(a) the type of personal data contained in the 13 insurance certificates and two letters was sensitive data; and

(b) the documents were not disposed of in a high traffic area such as a busy street or a shopping mall.

28 The Commissioner wishes to emphasise that organisations should take a very serious view of any instance of non-compliance under the PDPA, and the Commissioner urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commissioner will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

**SCHEDULE 1**

FULL LIST OF PERSONAL DATA IN THE PRUDENTIAL FOLDERS

1. Name of policyholder.
2. Client number.
3. NRIC number.
4. Age.
5. Date of certificate.
6. Policy number.
7. Cover start date.
8. Maturity date.
9. First premium due date.
10. Premium amount payable.
11. Name of life assured (all the 13 certificates listed the names of respective policyholders as the life assured).
12. Benefits.
13. Sum assured.
14. Cover start date.
15. Cover expiry date.
16. Premium.
17. Last premium due.

Grounds of Decision

## Re Aviva Ltd

## [2018] PDP Digest 245

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-1611-B0323
**Decision Citation**: [2018] PDP Digest 245; [2017] SGPDPC 14

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

11 October 2017

### BACKGROUND

1 Can an organisation fulfil its obligation to protect personal data by relying solely on its employees to perform their duties diligently? That is ultimately the question which the Commissioner had to determine in this matter.

2 The complaint which arose in this matter was that Aviva Ltd ("Organisation") had disclosed personal data without authorisation because it had mistakenly mailed to one of its policyholders ("First Policyholder") insurance documents which were meant for another policyholder ("Second Policyholder"). A family member of the First Policyholder lodged a complaint on 8 November 2016 and the office of the Commissioner proceeded to investigate the matter. The Commissioner's findings and the grounds of decision are set out below.

### MATERIAL FACTS

3 The Organisation is a multinational insurance company that offers various types of insurance plans to its policyholders.

4 On 1 November 2016, the Organisation was alerted to the data breach ("Incident") by a complaint from a family member of the First Policyholder. It undertook an internal investigation into the source of the

data breach, which was traced to its Processing Department. By way of background, the Organisation's Processing Department is in charge of, amongst other things, preparing follow-up letters that need to be sent to the Organisation's policyholders. This is done whenever the Organisation requires further administrative details or personal particulars from the policyholders as part of administering its insurance policies. In the event that there are any additional documents to be sent to a specific policyholder, *eg*, application forms or product summaries, staff ("processing staff") in the Processing Department would enclose the additional documents with the follow-up letter and place these in the same envelope. For each day of operation, there would be a total of four processing staff handling approximately 16 follow-up letters together with the enclosed additional documents.

5 The Organisation's investigations revealed that the Incident occurred when one of the processing staff erroneously enclosed the Second Policyholder's documents with follow-up letters addressed to the First Policyholder. This led to the First Policyholder receiving two envelopes from the Organisation. The first envelope ("Envelope 1") contained three documents; two documents were correctly addressed to the First Policyholder, but the third document was meant for the Second Policyholder. The second envelope ("Envelope 2") contained two documents; the first document was correct but the second document was an application form meant for the Second Policyholder.

6 The table below lists the documents contained in Envelopes 1 and 2 along with a description of the corresponding personal data that was disclosed without authorisation.

| | **Type of Documents** | **Personal Data Disclosed** |
|---|---|---|
| **Envelope 1** | 1. First Policyholder's MyShield "Request for further requirement(s)" letter<br>2. First Policyholder's MyShield Application Form<br>3. Second Policyholder's MyShield "Request for further requirement(s)" letter | *Second Policyholder*: name, address, policy plan type<br>*Second Policyholder's dependant*: full name |

| | | |
|---|---|---|
| **Envelope 2** | 1. First Policyholder's MyHealthPlus "Request for further requirement(s)" letter<br>2. Second Policyholder's MyShield Application Form | *Second Policyholder*: name, address, policy plan type, NRIC number, CPF account number, nationality, contact number, date of birth, gender, marital status, occupation, name of employer<br>*Second Policyholder's dependant*: full name, ID type, FIN, nationality, date of birth, gender, marital status, relationship to Second Policyholder |

7 The Organisation confirmed that at the time of the Incident, the team leader ("Team Leader") of the Processing Department did not perform any random checks on the work of the processing staff carrying out the enveloping process. In fact, the Organisation did not have in place any checks on the enveloping work of the processing staff at any time prior to the dispatch of the letters to policyholders.

8 Following its internal investigation, the Organisation revised its procedures for the enveloping process to include random checks by the Team Leader on any two of the envelopes processed during each day of operation.

## FINDINGS AND ASSESSMENT

### *Issue for determination*

9 The issue to be determined is whether the Organisation had, pursuant to s 24 of the Personal Data Protection Act 2012[1] ("PDPA"), put in place reasonable security arrangements to protect the personal data from unauthorised disclosure.

1 Act 26 of 2012.

10 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*

#### *Personal data was disclosed without authorisation*

11 It is not disputed that the information contained in Envelopes 1 and 2, which included details such as full name, NRIC number/FIN, Central Provident Fund ("CPF") account number, nationality, contact number, date of birth, gender, marital status, occupation and name of employer, falls within the definition of "personal data" under s 2 of the PDPA as it was possible to identify the two individuals (*ie*, the Second Policyholder and the Second Policyholder's dependant) from that information alone.

12 It is also not in dispute that the personal data of the Second Policyholder and the Second Policyholder's dependant contained in Envelopes 1 and 2 were disclosed mistakenly; the disclosure was therefore without authorisation. For completeness, the Commissioner notes that there was no unauthorised disclosure of the First Policyholder's personal data in the present case.

13 Based on the investigations carried out by the office of the Commissioner, 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.

#### *Personal data of sensitive nature should be safeguarded by higher level of protection*

14 The Commissioner assessed that the personal data of the Second Policyholder and the Second Policyholder's dependant in Envelopes 1 and 2 contained sensitive personal data. As detailed in the table at [6] above, the following sensitive personal data had been inadvertently disclosed: the Second Policyholder's insurance details, NRIC number, CPF account number, and the name and FIN of the Second Policyholder's dependant.

15 Furthermore, investigations found that Sections G ("Underwriting Options") and H ("Full Medical Underwriting Only") of the Second Policyholder's MyShield Application Form could have included sensitive medical information provided by the applicant. According to the Organisation, its usual practice was to have the MyShield Application Form filled up, including Sections G and H. However, in the present case, these sections were left blank as the Organisation had not obtained the relevant information. Had Sections G and H been pre-filled, additional sensitive medical information would have been disclosed to the First Policyholder due to the Incident. This was fortuitous for the Organisation and the individuals concerned (*ie*, the Second Policyholder and the Second Policyholder's dependant).

16 In addition, Section E ("Payment Details") of the Second Policyholder's MyShield Application Form was also left blank. If this section had been pre-filled, further sensitive personal data such as the Second Policyholder's credit card details (credit card number and expiry date) could have also been disclosed to the First Policyholder.

17 Even though there is no special category for sensitive personal data in the PDPA, past decisions and advisory guidelines have highlighted that certain types of personal data would typically be more sensitive in nature. These include: NRIC/Passport numbers;[2] personal data of a financial nature such as bank account details,[3] Central Depository account details, securities holdings, transaction and payment summaries;[4] names of the policyholder's dependants or beneficiaries, the sum insured under the insurance policy, the premium amount and type of coverage;[5] an individual's personal history involving drug use and infidelity;[6] sensitive medical conditions;[7] and personal data of minors.[8]

---

2 *Re JP Pepperdine Group Pte Ltd* [2017] PDP Digest 180 at [22]; *Re Singapore Telecommunications Limited* [2018] PDP Digest 148 at [26].

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

4 *Re Central Depository (Pte) Limited* [2017] PDP Digest 81 at [24].

5 *Re Aviva Ltd* [2017] PDP Digest 107 at [38].

6 *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188 at [9].

7 Personal Data Protection Commission, *Advisory Guidelines for the Healthcare Sector* (revised on 28 March 2017) at para 4.2.

8 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised on 28 March 2017) at para 8.12.

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 of sensitivity".[9] 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".[10] However, even though the Organisation's processing staff handles sensitive personal data of its policyholders in the course of their employment on a daily basis, the Organisation did not ensure that the sensitive personal data was accorded a high standard of protection, or that it was processed and mailed with particular care.

19 In adopting this view, the Commissioner agrees with the observations made by the Office of the Privacy Commissioner of Canada ("OPC") 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".[11] On the facts, the OPC found that the insurance company which was the subject of the report lost its policyholders' files containing sensitive personal data as the safeguards for the control and tracking of the insurance files at the time of the data breach incident were inadequate. The personal data leaked included: the individual's name; address; date of birth; height and weight; salary; signature; life insurance amounts (current coverage and requested coverage); medical information (including the

9 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at para 17.3.

10 PDPC, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* at para 2.2, first bullet point, p 5.

11 *PIPEDA Report of Findings #2014-003: Insurance Company Overhauls Its Security Safeguards Following Privacy Breach* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-003/>, first and second bullet points in the "Lessons Learned" section at p 2.

information declared on a paramedical examination and the results of a medical test); and an underwriter's notes and decision on the application.

*Unauthorised disclosure of personal data was result of the Organisation's failure to make reasonable security arrangements*

20 The Organisation represented that the enveloping error committed by its processing staff was an "isolated incident due to genuine oversight". However, upon a review of the Organisation's policies and processes, it was discovered that the Incident occurred due to the Organisation's lack of security arrangements in relation to the mailing of follow-up letters to its policyholders. In particular, the Organisation's processing standard operating procedures ("SOPs") were ineffective as a safeguard to protect the personal data; this was a systemic problem.

(i) The Organisation's processing SOPs were ineffective as safeguard

21 The Commissioner finds that the Organisation's enveloping process as disclosed in the processing SOPs at the time of the Incident did not incorporate reasonable security arrangements for the following reasons.

22 At the time of the Incident, each processing staff handling enveloping would check that he/she has enclosed the correct documents to the follow-up letters. No other staff would be responsible for further checks or ensuring that the correct documents had been enclosed with such letters before the envelopes were sealed and mailed out. When made aware of any errors by a staff member, the Team Leader would conduct a complete audit on the enveloping output of the staff in question for a period of one week.

23 The Organisation's processing SOPs at the time of the Incident did not include any second-level checks by the Team Leader on any of the follow-up letters that were prepared by the processing staff. This meant that there was no oversight of the enveloping process nor any supervision of the actions of each processing staff. As a matter of fact, the processing staff in charge of preparing and printing the follow-up letters and enclosing the additional documents was the only person checking the contents of the envelopes before they were mailed out to the policyholders.

24 This failure by the Organisation to put in place effective SOPs for the enveloping process was specifically highlighted in the *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* as follows:[12]

> Organisations that process and send documents or communications containing personal data should ensure that they have policies and procedures in place to prevent the sending of the documents or communications to the wrong recipients.
>
> For example, *organisations that prepare account statements (e.g. bank or insurance statements) to be mailed to individuals should take steps to ensure that the statements or the envelopes they are placed in*, or the emails they are attached in, *are not sent to the wrong recipients by* using incorrect postal or email addresses; or *enclosing the statement of another individual*.
>
> [emphasis added]

25 The same guide recommended the establishment of procedures for an organisation's staff to perform, as a best practice, "additional checks" following the processing, printing and sorting of documents to ensure that the destination information matches that of the intended recipient prior to mailing,[13] and that the right document containing the personal data is sent.[14] To be clear, the Commissioner is not setting down any rule that mandates organisations to establish procedures to perform "additional checks" in all cases. While it is recommended as a best practice, organisations should determine and adopt the most reasonable and appropriate policies and procedures given their specific circumstances.

26 In this case, the Commissioner finds that the absence of a second layer of basic checks to ensure that the letters and the enclosed documents were correctly addressed and mailed to the right policyholder pointed to a systemic weakness in the Organisation's processing SOPs and constituted a failure on the part of the Organisation to put in place reasonable security arrangements to protect the personal data.

---

12 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* at paras 1.1–1.2.

13 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* at para 2.1, second bullet point, p 4.

14 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* at para 2.1, fifth bullet point, p 4.

27 The processing SOPs were designed in such a way that the Organisation was entirely reliant on its processing staff to check that the follow-up letters had the correct documents enclosed. Although the Organisation claimed that it provided the necessary training and coaching to its processing staff to ensure their proficiency in performing their duties, the high risk of sensitive personal data being disclosed without authorisation was wholly unmitigated and dependent on the infallibility and consistency of the processing staff performing the enveloping work. The fact that the Organisation considered this to be an adequate form of protection is of concern, given that the Organisation is a well-established multinational organisation in the insurance business which handles large amounts of sensitive client personal data on a daily basis.

28 The Commissioner finds that it is insufficient for the Organisation to solely depend on its employees to carry out their duties diligently as a type of safeguard against an unauthorised disclosure of personal data. As observed in *Re Furnituremart.sg*,[15] it is "not enough for the Organisation to simply rely on its staff and employees to carry out their duties correctly for the protection of personal data". In that case, the organisation had represented that if its employees had carried out their job functions properly, by printing and sending the correct invoice to the correct recipient, there would not have been any data protection issue in the first place.[16] Such an argument was soundly rejected.

29 In the present case, investigations found that the processing staff in question had ten years of experience in enveloping work. The fact that this error was made by a highly experienced staff is telling. If a highly experienced staff made such a mistake, the probability of a less experienced staff committing a similar error is much higher. This adds further weight to the position that any SOPs or work process which solely relies on individual staff being infallible cannot constitute a reasonable security arrangement for the protection of personal data.

30 As such, the Commissioner is of the view that the Organisation failed to make reasonable security arrangements to protect the personal data having relied solely on the processing staff to diligently perform his/her functions to prevent the unauthorised disclosure of the personal data.

---

15 [2018] PDP Digest 175 at [21].

16 *Re Furnituremart.sg* [2018] PDP Digest 175 at [20].

(ii) The Organisation's data protection policy provided inadequate protection

31 For completeness, the Commissioner notes that at the material time, the Organisation had in place a general data protection policy ("PDPA Compliance Policy"). This was a high-level policy which listed out the nine data protection obligations in the PDPA and the responsibilities of employees. However, the PDPA Compliance Policy merely sets out some "dos and don'ts" concerning the protection obligation, examples of which follow:

> Do continue to comply with the various information security policies and standards issued by Aviva.
>
> …
>
> Do not share/disclose individual's personal data to anyone, including other staff, unless it is relevant and necessary for their performance of the duties.

These "dos and don'ts" did not provide sufficient instructions or guidance for the processing staff concerning their specific duties.

32 Security arrangements may take various forms. 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. However, in some cases, such policies may also serve as an administrative security measure to protect personal data.

33 Where a data protection policy is meant to serve as an administrative security measure to protect personal data, organisations should note the importance of providing employees with specific practical guidance on handling personal data in the course of their employment as set out in *Re Hazel Florist & Gifts Pte Ltd*:[17]

> The Commission notes that the Organisation has in place a Data Protection Policy. The Data Protection Policy merely restates the Organisation's data protection obligations in very general terms. The Organisation's Data Protection Policy does not provide the Organisation's employees with specific practical guidance on how to handle personal data in their day-to-day work or how to comply with section 24 of the PDPA. The Commission

17 [2018] PDP Digest 199 at [18].

> is, therefore, of the view that the Organisation's Data Protection Policy does not constitute a 'security arrangement' under section 24 of the PDPA ….

34 In the present case, the Organisation's PDPA Compliance Policy did not contain any mention of the preparation of the envelopes for the sending of follow-up letters to the Organisation's policyholders, nor any reference to the checking or verification of the enclosed documents. Whilst there was some attempt to elaborate on the protection obligation through the provision of basic "dos and don'ts", the PDPA Compliance Policy did not go further to provide practical guidance on how an employee could comply with s 24 of the PDPA in the course of his/her daily work. Due to this lack of specificity and detail, the Commissioner is not satisfied that the PDPA Compliance Policy constituted a reasonable security arrangement under s 24 of the PDPA.

*Conclusion of Commissioner's findings*

35 Considering the level of sensitivity of the personal data that the Organisation handled on a daily basis with regard to follow-up letters and the enclosed documents, the Organisation did not put in place reasonable security arrangements to protect the personal data. The absence of any second-level checks in the Organisation's processing SOPs at the material time and the lack of any other form of security arrangement to prevent the erroneous mailing of one policyholder's documents to another amounted to extremely weak internal work process controls and fell far short of the standard of protection required for such sensitive personal data.

36 In consideration of the above, the Commissioner is not satisfied with the Organisation's claim that the unauthorised disclosure was caused by an isolated, one-off case of human error. The Commissioner finds that the Organisation failed to make reasonable security arrangements to protect the personal data in its possession or under its control, in breach of s 24 of the PDPA.

## REMEDIATION ACTIONS TAKEN BY THE ORGANISATION

37 The Commissioner notes that after the data breach incident, the Organisation counselled the staff in question, carried out an audit on the staff's enveloping output for one week, and revised its SOPs to add an additional layer of checks by the Team Leader of the enveloping process.

Pursuant to the revised SOPs, the Team Leader would, on each day of operation, randomly check two envelopes whenever there are documents to be enclosed with the follow-up letters to ensure that the personal data of its policyholders and their dependants are not mistakenly sent to others. Also, the week-long audit by the Team Leader on the processing staff who makes a mistake has now been operationalised as part of the SOPs. The relevant portions from the revised SOPs (which took effect from 3 December 2016) are reproduced below for reference:

> **7. Verification of Data Creation and Processing**
> Cases created in AS400 will be checked randomly by the respective team leaders.
>
> Each team leader will check 5 cases of data creation per day. The team leader will ensure that he/she checks at least a case for each team member. The cases checked will be updated in an excel spreadsheet in our common drive.
>
> Should there be new team member, his/her mentor will check his/her work thoroughly until he/she is able to deliver the work accurately. This process is independent from the existing staff verification.
>
> *Each team leader will check 2 cases of enveloping randomly per day. If error is detected, the team leader will conduct 100% audit on the erred staff enveloping output for a period of one week*. The cases checked will be updated in the excel spreadsheet in our common drive.
>
> [emphasis added]

38 Given the estimated average workload of 16 follow-up letters per day, a random check of two envelopes amounts to a sample size of about 10%.

39 The Commissioner has not reviewed the Organisation's considerations in deciding on the sample size and is not making any opinion on the revised SOPs as it is unnecessary to do so for the purposes of making a breach finding against the Organisation.

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 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.

42 With this in mind, it is advisable for the Organisation to monitor the effectiveness of its revised SOPs and to make further revisions as necessary.

43 For completeness, the Commissioner notes that the Organisation also sent an apology letter to the First Policyholder and retrieved the wrongly delivered documents. As for the Second Policyholder, the Organisation sent an apology letter along with shopping vouchers worth $100.

## DIRECTIONS

44 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 $1m as the Commissioner thinks fit.

45 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:

(a) the personal data disclosed, especially the Second Policyholder's NRIC number; CPF account number; and the full name and FIN of the Second Policyholder's dependant, 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;

(c) the Organisation had co-operated fully with investigations and was forthcoming in admitting its mistake;

(d) the Organisation had notified the affected victim, *ie*, the Second Policyholder, of the data breach incident, and offered an apology and shopping vouchers, and had also made arrangements to retrieve the wrongly delivered documents from the First Policyholder;

(e) the unauthorised disclosure of personal data was limited to possibly three individuals, comprising of the First Policyholder and the First Policyholder's nuclear family; and

(f) there was no evidence to suggest that there had been any actual loss or damage resulting from the unauthorised disclosure.

46 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 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 $6,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

47 The Commissioner urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. Appropriate enforcement action against non-compliant organisation(s) will be taken.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re M Stars Movers & Logistics Specialist Pte Ltd

## [2018] PDP Digest 259

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1612-B0418
**Decision Citation**: [2018] PDP Digest 259; [2017] SGPDPC 15

***Consent Obligation*** *–Disclosure of personal data without consent*
***Openness Obligation*** *– Failure to appoint data protection officer*
***Openness Obligation*** *– Lack of data protection policies and practices*

15 November 2017

### BACKGROUND

1 This case highlights the risks that organisations face when they fail to develop and implement policies, practices and procedures to protect personal data when communicating with their customers or other individuals through social media.

2 In this matter, a customer ("Complainant") of the organisation ("Organisation"), which provides professional moving services, alleged that the Organisation had disclosed her personal data on its Facebook page without her consent.

3 The findings and grounds of decision based on the investigations carried out in this matter are set out below.

### MATERIAL FACTS

4 Sometime in December 2016, the Complainant engaged the Organisation's professional moving services. The Complainant voluntarily provided her name, mobile number and residential addresses (*ie*, the addresses where the items were to be picked up and delivered to) to the Organisation to provide the services.

5 Dissatisfied with the allegedly unsatisfactory services provided by the Organisation, the Complainant left a negative review in a public post on the Organisation's Facebook page. Amongst other things, there was a disagreement as to when the Organisation was required to return the $100 deposit to the Complainant.

6 The Organisation publicly responded to the Complainant's review in the comment section of the Complainant's post on its Facebook page. In its response, the Organisation identified the Complainant by her English name and surname ("name") and residential address (collectively referred to as "Personal Data") and informed the Complainant that she would receive her deposit once she returned the carton boxes that the Organisation had previously provided to her to assist her in moving her belongings.

7 Shortly after the Organisation had disclosed the Complainant's Personal Data on its Facebook page, the Complainant sent the Organisation a private Facebook message requesting the immediate removal of her residential address from the Organisation's Facebook page. The Organisation denied any wrongdoing and refused to remove the Complainant's address from its Facebook page until it was advised to do so by the office of the Commissioner.

8 The Organisation's explanation was that it had disclosed the Complainant's name and residential address in its response to identify the Complainant "to ensure that [it was] refunding the money of $100 [*ie*, the deposit] to the correct person".

9 The Organisation admitted in the course of the investigations that it was not aware of the Personal Data Protection Act 2012[1] ("PDPA"). Consequently, it did not appoint a data protection officer ("DPO") nor did it implement any data protection policies or guidelines.

## FINDINGS AND BASIS FOR DETERMINATION

10 The issues for determination are:

(a) whether the Organisation had disclosed the Complainant's Personal Data without consent or authorisation; and

1 Act 26 of 2012.

(b) whether the Organisation had complied with its obligations under ss 11 and 12 of the PDPA.

11 The information disclosed by the Organisation is clearly "personal data" within the meaning of s 2(1) of the PDPA as the Complainant could be identified from the information disclosed. The Organisation did not dispute this.

### *Whether the Organisation had disclosed Complainant's personal data without consent or authorisation*

12 Subject to certain exceptions,[2] 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").

13 An individual may, in some circumstances pursuant to s 15 of the PDPA, be deemed to have consented to the collection, use and disclosure of his/her personal data where he/she voluntarily provided the personal data and it is reasonable that he/she would voluntarily provide the data.[3]

14 The Complainant engaged the Organisation to move her belongings to her new home. It is in this context that the Complainant provided her Personal Data to the Organisation, so that the Organisation would know the location from which to pick up the Complainant's belongings and the delivery address. No evidence has been adduced of the Complainant consenting to the disclosure of the Personal Data on the Organisation's public Facebook page. Further, the Deputy Commissioner finds that the Complainant is not deemed to have consented to the said disclosure as the two limbs for making a finding of deemed consent under s 15(1) of the PDPA have not been made out. In this context, it cannot be said that this manner of disclosure of the Complainant's Personal Data by the Organisation in its response to her review on its Facebook page was within the Complainant's reasonable contemplation.

15 The Organisation's explanation that it replied to the Complainant's Facebook post with the Personal Data as it wanted to confirm the identity

2 Pursuant to s 17 of the Personal Data Protection Act 2012 (Act 26 of 2012) read with the Second, Third and Fourth Schedules to the Act.

3 Personal Data Protection Act 2012 (Act 26 of 2012) s 15.

of the Complainant does not address the reason the Organisation publicly disclosed the Personal Data on its Facebook page. The Organisation's objective of ensuring the identity of the Complainant was not better served by disclosing the Personal Data *publicly* on its Facebook page instead of *privately* communicating with the Complainant directly. There was no legitimate reason for disclosing the Personal Data to third parties. Given the Organisation's admission of its lack of awareness of the PDPA and the obligations it imposes, it is more likely than not, that the Organisation disclosed the Personal Data simply for convenience without further consideration.

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 excuse its breach of the PDPA. The data protection provisions of the PDPA took effect on 2 July 2014[4] 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.

17 It is apropos to address an issue which commonly arises in the context of an organisation's communications through its commercial social media page. When is it ever acceptable to disclose personal data when an organisation is responding to public comments? It is unlikely that the terms of *ex ante* consent or scope of deemed consent can cover such disclosures.

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.

---

4 Personal Data Protection Act 2012 (Commencement) Notification 2014 (S 361/2014).

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 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 (in this case the dispute was the Complainant's alleged dissatisfaction with the services provided by the Organisation). Second, the disclosure may sometimes be justified by exceptions to consent. For example, disclosures in the course of the organisation's investigations into alleged breaches of agreement or into conduct that may give rise to tortious claims. Disclosures in reliance on exceptions to consent will nevertheless have to be limited in scope in order to achieve the purposes of the applicable exception. Third, even in the absence of consent (whether express or deemed) or an applicable exception, it may nevertheless be objectively reasonable for the organisation to disclose personal data in response to allegations made against it. Section 11(1) of the PDPA exhorts organisations in discharging its responsibilities under the PDPA to "*consider* what a reasonable person would consider appropriate *in the circumstances*" [emphasis added]. This requires fact-specific analysis and the burden is on the organisation to justify that the circumstances were atypical, the disclosure was warranted and its actions were reasonable.

20 In the present case, the Complainant had posted a lengthy complaint on the Organisation's Facebook page, amounting to approximately 500 words. The Organisation responded in three separate posts. Having perused the explanations and considered the context of the disclosure of the Personal Data, it cannot be said that the disclosure of the Personal Data had any nexus to the allegations and explanations. Hence, the disclosure in its response was clearly disproportionate. The Organisation's response was not made in the context of an *investigation* into a civil dispute (although one patently existed), nor did it fall within any other exception. Finally, the Organisation's disclosure was unwarranted and unreasonable as it was made, more likely than not, for convenience without further consideration (see [15] above).

21 Given the foregoing, the Deputy Commissioner finds that the disclosure of the Personal Data on the Organisation's Facebook page was made in breach of its Consent Obligation under the PDPA.

***Whether the Organisation had complied with its obligations under sections 11 and 12 of the Personal Data Protection Act***

22 Section 11(3) of the PDPA requires an organisation to designate one or more individuals (*ie*, the DPO) to be responsible for ensuring compliance with the PDPA and s 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 (collectively, "Openness Obligation").

23 During the investigations, the Organisation admitted that it was not aware of the PDPA and, consequently, its data protection obligations[5] under the PDPA. The Organisation also confirmed that, at the material time, it did not implement any data protection policies or practices, nor did it appoint a DPO.

24 In the circumstances, the Deputy Commissioner finds that, by its own admission, the Organisation failed to meet its obligations under ss 11(3) and 12(*a*) of the PDPA. In this regard, the Deputy Commissioner repeats his comments made at [16] 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.

*Data protection policies*

25 The Deputy Commissioner takes this opportunity to highlight 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.

26 In this regard, the Deputy Commissioner repeats the Commissioner's guidance in *Re Aviva Ltd*[6] 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 section 12 of the PDPA are generally meant to increase awareness and ensure accountability of the organisation's obligations under the PDPA ….

5 Under Pts III–VI of the Personal Data Protection Act 2012 (Act 26 of 2012).

6 [2018] PDP Digest 245 at [32].

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 (*eg*, communications through social media).

29 A general data protection policy is, however, not the be all and end all of data protection. Specific practices, processes, procedures and measures need to be put in place by organisations to protect personal data. In this regard, the Deputy Commissioner agrees with the following comments made by the Office of the Privacy Commissioner of Canada's decision in the case of *Google Inc WiFi Data Collection*[7] on the necessity to put in place real and effective measures to ensure an organisation's accountability for the personal data it handles:

> The obligation that organizations must have in place the proper practices, as a matter of accountability, concords with a growing international recognition that the protection of personal information requires real and effective measures. It is this Office's view that organizations need to implement appropriate and effective measures to put into effect the principles and obligations of the Act, including effective compliance and training programs, as an essential part of ensuring that organisations remain accountable for the personal information they collect, use or disclose.

30 Organisations with a social media or other online presence (*eg*, social media forums), particularly those that rely on such platforms to communicate with its customers, ought to develop appropriate policies,

---

7 *PIPEDA Report of Findings #2011-001: Google Inc WiFi Data Collection* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/> at [71].

practices and procedures that amply address the risks of disclosing personal data on social media or other online sites. Together, these policies, practices and procedures should seek to (a) ensure that staff who communicate through an organisation's social media account or similar platforms are aware of the organisation's data protection obligations and the importance and need to protect personal data; (b) crystallise the organisation's position on the circumstances in which it may be appropriate to disclose personal data on these platforms, for example, disclosures to which individuals have already consented; (c) ensure that the organisation maintains an appropriate level of control on the content posted on these platforms (*eg*, by limiting the number of staff who are allowed to post and placing conditions on these staff such as requiring them to undergo relevant data protection training); (d) crystallise the organisation's retention rules in respect of posts on such platforms; and (e) provide an avenue to escalate issues or queries to the appropriate function or role within the organisation.

31 A well-informed DPO who is familiar with data protection law and practice, should be able to ensure that these policies, practices and procedures are updated to guide members of staff on the appropriate conduct when using such platforms as means of corporate communications, including with customers, and also provide guidance as to when communications commenced on public fora ought to continue in more private channels.

*Data protection officer*

32 The above paragraph segues appropriately into a discussion of the requirement and role of the DPO.

33 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. This will ensure that the board of directors and C-level executives are cognisant of the risks. 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. If not one of the C-level executives, the DPO should have at least a direct line of communication to them. This level of access and empowerment will provide the DPO with the necessary wherewithal to perform his/her role and accomplish his/her

functions. The DPO need not – and ought not – be the sole person responsible for data protection within the organisation. Properly implemented, data protection policies will touch most, if not all, parts of an organisation. Every member of staff has a part to play. The DPO is the person within an organisation responsible for implementing the policies and practices, just as the board and C-level executives are ultimately accountable to shareholders and owners for any failure to comply.

34 The responsibilities of a DPO include, but are not limited to:[8]

> (a) ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data, including processes and formal procedures to handle queries and/or complaints from the public;
> (b) fostering a data protection culture and accountability among employees and communicating personal data protection policies to stakeholders;
> (c) handling and managing personal data protection related queries and complaints from the public, including making information about the organisation's data protection policies and practices available on request to the public;
> (d) alerting management to any risks that might arise with regard to personal data; and
> (e) liaising with the Commissioner on data protection matters, if necessary.

35 In this regard, the Deputy Commissioner agrees with the position adopted in the Canadian Joint Guidance Note[9] on the role and responsibilities of a DPO (or privacy officer in the Canadian context) in an organisation:

> Organizations must appoint someone who is responsible for the privacy management program.

---

8 Personal Data Protection Commission, *Data Protection Officers* <https://www.pdpc.gov.sg/organisations/data-protection-officers> at para 4.

9 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* <https://www.oipc.bc.ca/guidance-documents/1435> at p 7.

> *Whether this person is a C-level executive of a major corporation or the owner/operator of a very small organization, someone must be assigned responsibility for overseeing the organization's compliance with applicable privacy legislation.* Other individuals may be involved in handling personal information, but *the Privacy Officer is the one accountable for structuring, designing and managing the program, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up*. Organizations should expect to dedicate some resources to training the Privacy Officer. The Privacy Officer should establish a program that demonstrates compliance by mapping the program to applicable legislation. It will be important to show how the program is being managed throughout the organization.
>
> The Privacy Officer will play many roles with respect to privacy. S/he will:
>
> - establish and implement program controls;
> - coordinate with other appropriate persons responsible for related disciplines and functions within the organization;
> - be responsible for the ongoing assessment and revision of program controls;
> - represent the organization in the event of a complaint investigation by a privacy commissioner's office; and
> - advocate privacy within the organization itself.
>
> This last role is as crucial as the others. Organizations face competing interests and privacy compliance is one program of many. *Privacy, however, is more than a balancing of interests. Privacy should be seen in terms of improving processes, customer relationship management, and reputation. Consequently, the privacy management program's importance must be recognized at all levels.*
>
> [emphasis added]

36 Again, while the quote above is in respect of a privacy officer, it is equally applicable in the context of a DPO under the PDPA notwithstanding the differences between privacy and data protection.

37 From the foregoing, it is clear that regardless of the size of an organisation, the DPO plays a vital role in building a robust data protection framework to ensure the organisation's compliance with its obligations under the PDPA.

## DIRECTIONS

38 Having found that the Organisation is in breach of ss 11(3), 12(*a*) and 13 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. This may include directing the Organisation to pay a financial penalty of such amount not exceeding $1m.

39 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 was limited to the Complainant's name and residential address; and

(b) the Organisation's breach of the Consent Obligation was due to its lack of awareness of the Organisation's obligations under the PDPA.

40 The Deputy Commissioner has decided to issue the following directions to the Organisation:

(a) to put in place a data protection policy and internal guidelines to comply with the provisions of the PDPA within 60 days from the date of this direction;

(b) to appoint a DPO within 30 days from the date of this direction; and

(c) to inform the office of the Commissioner of the completion of each of the above directions within one week of implementation.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re BHG (Singapore) Pte Ltd

## [2018] PDP Digest 270

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1701-B0440
**Decision Citation**: [2018] PDP Digest 270; [2017] SGPDPC 16

***Protection Obligation*** *– Unauthorised access to personal data – Reasonable security arrangements*

15 November 2017

### BACKGROUND

1 An organisation's requirement to prevent the unauthorised disclosure of or access to personal data under the Personal Data Protection Act 2012[1] ("PDPA") is not absolute in nature, in that the obligation is not automatically breached upon the occurrence of a data leak. This case provides a classic example of the application of this principle.

2 The complainant ("Complainant"), a customer of the organisation ("Organisation"), discovered that she had accessed the online BHG loyalty card account of another customer ("Customer V") of the Organisation after she changed the password to what she thought was her BHG loyalty card account. As a result, the name, gender, date of birth, race, marital status, income group (based on income range) and residential address (collectively referred to as "Personal Data") of Customer V was inadvertently accessed by the Complainant.

### MATERIAL FACTS

3 The Organisation is a department store with various outlets in Singapore. It operates a loyalty card programme called the BHG Rewards

1 Act 26 of 2012.

Card programme for customers who fulfil certain criteria (such as a minimum spend within an allocated period in order to qualify for the programme). Customers issued with a BHG Rewards Card earn points on purchases made at the Organisation's stores depending on the amount spent. These points can then be used to redeem shopping vouchers for use at the Organisation's stores. There are also other benefits in joining the BHG Rewards Card programme, such as exclusive promotions and activities.

4 Both the Complainant and Customer V met the prerequisites for joining the BHG Rewards Card programme and applied to join the programme on 26 December 2016.

### *BHG Rewards Card registration process*

5 Customers who wish to register for the BHG Rewards Card programme are required to make their application at the customer service counter ("CSC") at the Organisation's stores. The registration is generally done by the customer on the Organisation's electronic tablets by inputting certain personal data into an electronic registration form. Amongst other personal details, the customer is required to provide his mobile phone number and e-mail address. The customer's mobile phone number is used as the default user ID to access the customer's BHG Rewards Card account online.

6 When the customer is done keying the required personal data into the electronic form, an employee of the Organisation at the CSC will assist the customer to submit the details. This would generate a membership number and automatically "refresh" the screen; the details keyed in by the customer would no longer be displayed. The membership number is used as the default password to access the customer's BHG Rewards Card account online.

7 As a precaution, the employee assisting the customer with the registration is required to also manually refresh the screen on the electronic tablet by closing the registration form and opening a fresh instance of the form before using the tablet again. The manual "refresh" procedure is also to be undertaken if there are any technical problems in using the electronic tablet for the registration.

8 The electronic tablet was also programmed to purge all the details keyed into the form if there was inactivity for about 30 seconds.

### *Accessing customer's online loyalty card account*

9 As set out above at [5] and [6], a customer may access his BHG Rewards Card account online by using his mobile phone number as his user ID and the membership number as his password. If the customer forgets his membership number, he can request for a new password to be sent to his e-mail address which the customer would have keyed in when registering for the loyalty card.

### *Registration of Complainant's and Customer V's accounts were affected because of technical problems with electronic tablets at Jurong Point store*

10 On 26 December 2016, both the Complainant and Customer V visited the Organisation's Jurong Point store and applied to join the BHG Rewards Card programme. On the same day, the assistant retail manager ("Assistant Retail Manager") of the Jurong Point store who was tasked to assist customers in registering their BHG Rewards Card accounts had experienced technical problems with the two electronic tablets used for registration. She informed the relevant department of the technical issues.

11 When the Complainant approached her for assistance in registering for the BHG Rewards Card, the Assistant Retail Manager handed the Complainant one of the electronic tablets ("tablet 1") to input the required details into the electronic registration form. However, technical issues caused the electronic tablet to "hang" or become unresponsive a few times when the Complainant tried to input the required details. The Assistant Retail Manager decided to abandon the electronic registration and instead asked the Complainant to fill in a physical registration form and subsequently issued the Complainant with a temporary BHG Rewards Card together with a membership number.

12 According to the Organisation, the technical issues experienced in typing the details into the electronic registration form was likely due to one or both of the following:

(a) The postal code directory uploaded onto the Organisation's registration system was not up to date. The system failed to recognise

the postal code entered by the Complainant as her postal code was not included in the version which the Organisation was using at the time, causing the electronic tablet to "hang".

(b) Poor Wi-Fi connection on the day meant that the electronic tablet would have had difficulty connecting to the Organisation's registration system.

13 Customer V who was at the CSC at the same time as the Complainant was also having problems with the other electronic tablet ("tablet 2") which he was using to register for the BHG Rewards Card. A part-time employee ("Employee A") of the Organisation who was also stationed at the CSC was assisting Customer V. Employee A asked Customer V to try using tablet 1 which was last used by the Complainant instead. However, when Employee A handed tablet 1 to Customer V, the screen was not refreshed properly and continued to display at least some of the Complainant's personal data. It is not known how much of the Complainant's personal data continued to be displayed, but as will be explained in the next paragraph, at least the mobile phone number and e-mail address of the Complainant continued to be displayed.

14 Customer V proceeded to key the required details into the electronic registration form using tablet 1. However, Customer V's BHG Rewards Card account was registered with the Complainant's mobile phone number and e-mail address. This is likely because the Complainant's mobile phone number and e-mail address continued to appear on the form while Customer V was keying in his details. However, it is not clear why Customer V left the Complainant's particulars on the form or why he did not alert Employee A or any other employee to the fact that the Complainant's details were still visible on the form. Customer V was able to complete and submit his electronic registration and was issued a BHG Rewards Card account number.

### *Complainant accesses Customer V's account information*

15 On the same day, the Complainant downloaded the app ("BHG App") which allowed customers to access their BHG Rewards Card accounts and tried to log into her account. As explained above at [9], the default login credentials to the BHG App were the mobile phone number registered with the customer's account (default user ID) and the customer's membership card account number (default password). Given that the

Complainant's mobile phone number was tied to Customer V's BHG Rewards Card account number, the login credentials did not match and the Complainant was denied access to her account.

16 The Complainant, therefore, then submitted a password reset request to the Organisation by providing her mobile phone number and e-mail address in accordance with the Organisation's password reset process. This password reset was successfully activated because the Complainant's mobile phone number and e-mail address matched the details with which Customer V's account was registered. Once the password was reset, the Complainant managed to log into what she thought was her account. However, once she accessed the account, the Complainant realised that, except for her mobile phone number and e-mail address, the account contained the Personal Data of Customer V. The Complainant alerted the Organisation and this office of this unauthorised access.

## COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

17 The issue to be determined in this case is whether the Organisation complied with its protection obligation pursuant to s 24 of the PDPA and implemented reasonable security arrangements to prevent the unauthorised access to the Personal Data.

18 For completeness, the Deputy Commissioner is satisfied that the two preconditions to the application of s 24 as stated in *Re Hazel Florist & Gifts Pte Ltd*[2] – that BHG (Singapore) Pte Ltd is an organisation within the meaning of the PDPA and is in possession or control of the Personal Data – have been met and it is not in dispute that s 24 applies in this matter.

19 It is also not disputed that the information to which the Complainant had access, as set out above at [2], falls within the definition of "personal data" under s 2 of the PDPA as it was possible to identify Customer V from that information alone.

20 Further, it is not disputed that the Complainant was not supposed to have access to the Personal Data; the access was therefore without authorisation.

---

2 [2018] PDP Digest 199 at [8]–[9].

***Whether the Organisation was in breach of section 24 of the Personal Data Protection Act***

*Security arrangements implemented by the Organisation to prevent unauthorised access to Personal Data*

21 The investigations by this office found that the following security arrangements were implemented by the Organisation to prevent unauthorised access to the Personal Data:

(a) *Automated "refresh" of the screen*: The electronic registration system was programmed such that the screen on the electronic tablet would "refresh" once the electronic registration form was successfully submitted. This would mean that the personal data keyed in by the customer would be deleted from the registration form on the electronic tablet and would no longer be displayed on the screen.

(b) *Manual "refresh" of the screen*: The Organisation's staff assisting customers with their BHG Rewards Card registration at the CSC are required to "refresh" the system on the electronic tablet before they hand the electronic tablet to the next customer. This manual "refresh" is done by closing the open instance of the electronic registration system and opening a fresh instance of the system. The manual "refresh" is also required to be done whenever the staff encounter a technical issue with the electronic tablet. This manual "refresh" process and general guidance on handling customer's personal data was communicated to both the Assistant Retail Manager and Employee A through mandatory training programmes. The Assistant Retail Manager received on-the-job training sessions three days a week over a period of ten months, which included training in the electronic registration of customers' BHG Rewards Card applications. Additionally, the Assistant Retail Manager was also trained by the Organisation's in-house trainer on the electronic registration process. Employee A also received on-the-job training on the electronic registration process. Both staff completed the training before the incident occurred.

(c) *Login credentials for the BHG App*: The default login credentials are set as a customer's mobile phone number (user ID) and membership card account number (password). Each customer who registers for the BHG Rewards Card will be assigned a unique 16-digit membership card account number that is automatically

generated from the Organisation's system once a registration is completed.[3]

(d) *Authentication for password reset requests*: A customer may request a password reset by providing the customer's mobile phone number and e-mail address, as a form of verification and authentication by the system before a password reset is allowed.

(e) *Automatic time-out*: The electronic registration form is programmed to time out after about 30 seconds of inactivity, after which all the personal data keyed into the electronic registration form will be deleted.

*Unauthorised access was caused by confluence of events and circumstances that would have been difficult to foresee*

22 The investigation determined that the unauthorised access was caused as a result of the following events and circumstances:

(a) The Complainant's electronic registration could not be completed meaning that the Complainant's data was not automatically cleared from the electronic registration form.

(b) Employee A did not correctly "refresh" tablet 1. In this regard the Assistant Retail Manager had handed tablet 1 to Employee A and asked her to perform a manual "refresh". The Assistant Retail Manager had on numerous occasions during the same day asked Employee A to perform the manual "refresh" and checked that it was done properly. On this occasion, the Assistant Retail Manager, given that Employee A had performed the manual "refresh" properly on all of the earlier occasions and that the CSC was very busy during this peak period, trusted Employee A to perform the manual "refresh" and did not check if it was done.

(c) Customer V did not alert either Employee A or the Assistant Retail Manager and continued with his registration despite the

3 See *Re ABR Holdings Limited* [2017] PDP Digest 117 at [15]–[16], where it was held that the organisation's use of a single string of numbers as the only security arrangement to identify and authenticate access to personal data may constitute reasonable security arrangements depending on the sensitivity of the personal data protected only if the number is unique, unpredictable and reasonably well protected.

Complainant's data continuing to be displayed. This, to the Deputy Commissioner's mind, is one of the baffling features of this case. Customer V did not provide his own mobile phone number and e-mail address but left the contact details of someone else in an online form that he was filling out himself. There is a certain degree of responsibility that each person should exercise over his own personal data, even if this is no more than contact details that are freely disseminated. Customer V's oversight in this case was a key mistake in an unfortunate sequence of events.

(d) Of all the fields of personal data keyed in by the Complainant, only the Complainant's e-mail address and mobile telephone number were included in Customer V's BHG Rewards Card account. Unfortunately, this was the exact information that allowed the inadvertent unauthorised access to the Personal Data.

23 The above explanation for the cause of the unauthorised access to the Personal Data shows that it was caused by a confluence of events and circumstances. It is clear that the Organisation recognised its obligation to protect its customers' personal data and addressed its mind to the various scenarios in which the personal data of a BHG Rewards Card applicant could be disclosed or accessed without authorisation during the registration process. It recognised that the automatic "refresh" could potentially fail and as such the Organisation required its staff to perform a manual "refresh" as well. The requirement to perform a manual "refresh" and the process for doing so was communicated clearly to all staff assisting at the Organisation's CSCs. Besides the training programmes the Assistant Retail Manager and Employee A underwent, the senior staff at the CSCs also supervise the other employees in performing the manual "refresh" on a day-to-day basis. This supervision, which the Assistant Retail Manager performed during the day of the incident, served as another line of security during the registration process.

24 Finally, access to a customer's BHG Rewards Card account would only be granted if the user attempting to access the account knew the said customer's (a) mobile phone number; and (b) the rewards card number or, in the case of a password reset request, the e-mail address.

25 The question that remains is whether the above arrangements were reasonably appropriate in protecting the Personal Data from unauthorised access. In answering this question, the Deputy Commissioner notes that the

wording of s 24 does not require an organisation to provide "an absolute guarantee"[4] for the protection of personal data in its possession or under its control and takes reference from the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* which recommends that:[5]

> Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected (*e.g.* physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

26 In this case, the Personal Data, while important, were essentially demographic and contact details. In such circumstances, would the Organisation be required to implement security arrangements in addition to those that were already implemented at the time of the incident? Looking at the security arrangements that were implemented at the material time, it is clear that the automatic "refresh", the manual "refresh" and the supervisory checks would have all separately prevented the unauthorised access.

27 In this incident, however, the circumstances were such that each of these arrangements failed individually. First, both tablets 1 and 2 were not functioning properly during the day. Second, the Complainant's registration could not be submitted electronically and hence the electronic registration form was not refreshed automatically. Third, Customer V could not complete his registration with the tablet he was initially given and instead used tablet 1 immediately after the Complainant's failed attempt to register using tablet 1. Fourth, Employee A did not properly perform a manual "refresh" of tablet 1 as was the process stipulated by the Organisation and as requested by the Assistant Retail Manager. This was despite Employee A performing the manual "refresh" properly numerous times during the day. Fifth, the Assistant Retail Manager failed to check that the manual "refresh" was done properly. Sixth, Customer V did not alert the staff at the CSC that the Complainant's personal details continued to appear on the electronic registration form, and did not replace the details but continued to submit his application with another person's mobile

---

4 *Re Tiger Airways Singapore Pte Ltd* [2018] PDP Digest 166 at [17].

5 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at para 17.2.

phone number and e-mail address as part of his registration details. Seventh, the only details of the Complainant with which Customer V registered his account were the exact details which were required to allow the Complainant access to the Personal Data.

28 Looking at the above, it is the Deputy Commissioner's view that this incident resulted from an unusual confluence of circumstances. Also, nothing in the investigations pointed to a systemic problem that caused the unauthorised access to the Personal Data. This appeared to be a one-off incident that would have been difficult to foresee. Therefore, the Deputy Commissioner is of the view that the security arrangements implemented by the Organisation to prevent the unauthorised access to the Personal Data were reasonable in the circumstances.

## REMEDIAL ACTION BY THE ORGANISATION

29 The Organisation launched an internal investigation into the unauthorised access to the Personal Data when the Complainant alerted it to the incident. The Organisation undertook the following remedial actions:

(a) *Responding to the affected individual*: The Organisation informed Customer V of the unauthorised access to the Personal Data and created new membership accounts for the Complainant and Customer V with the correct sets of personal data.

(b) *Remedial action concerning staff training*: The Organisation scheduled refresher data protection training for all CSC staff and issued a warning to the Assistant Retail Manager for her contributory role in the unauthorised access to the Personal Data in order to deter the other CSC staff from deviating from the SOPs.

(c) *Remedial action concerning technical safeguards*: The Organisation instructed and scheduled its IT personnel to verify the setting of its electronic tablets at all of its outlets and carry out extensive checks on all its electronic tablets to ensure proper function and correct settings. It also informed its vendor of the technical problems faced in using the tablets. The Organisation also purchased and uploaded into its electronic registration system the most updated version of the postal code directory to prevent the same problem from recurring and provided every outlet with a new 4G Wi-Fi dongle to ensure a stable network connection.

(d) *Further remedial action on operational processes*: The Organisation instructed its consultant to review the membership registration process to consider only collecting names, mobile phone numbers and addresses in future registrations (with the collection of other personal data optional) and to study a potential revision of the verification process which grants customers access to their membership accounts via the BHG App, including stronger authentication checks before a customer is able to request for a password reset.

## CONCLUSION

30 On balance, the Deputy Commissioner concludes that the Organisation implemented security arrangements of a reasonable standard to protect the personal data in its possession and under its control, and therefore makes a finding of no breach in the present case. Further, the Deputy Commissioner finds that the remedial actions undertaken by the Organisation satisfactorily address the residual harm caused by the unauthorised access to the Personal Data. There is, therefore, no need for the Deputy Commissioner to issue any directions in this case.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re Social Metric Pte Ltd

## [2018] PDP Digest 281

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-160-A712; DP-1604-A713
**Decision Citation**: [2018] PDP Digest 281; [2017] SGPDPC 17

***Data Protection Provisions coming into force and effect***
***Obligations of organisation and data intermediary*** *– Data intermediary taking on role and responsibilities of organisation*
***Protection Obligation*** *– Disclosure of personal data – Insufficient technical and administrative security arrangements*
***Retention Limitation Obligation*** *– Purpose for which personal data was collected no longer served by retaining data – Retention no longer necessary for legal or business purposes*

27 November 2017

### BACKGROUND

1 This case involves a company which, as part of its social media marketing campaigns conducted for and on behalf of its clients, created webpages containing the personal data of its clients' customers; and subsequently failed to remove those webpages from the World Wide Web, even after the social media marketing campaigns were over.

2 A complaint was made to the Personal Data Protection Commission ("Commission") regarding the unauthorised disclosure of personal data on these webpages on the World Wide Web. The Commissioner undertook an investigation into the matter, and the Commissioner sets out his findings and decision on the matter below.

### MATERIAL FACTS AND DOCUMENTS

3 Social Metric is a digital marketing agency that provides social media marketing services. As part of these services, Social Metric would collect

personal data of its clients' customers for various purposes, for example, as a form of customer engagement, or to analyse the customer demographics, amongst other things.

4 For the webpages in question, Social Metric had created nine webpages ("Webpages") for various social media contests that Social Metric conducted for and on behalf of its clients. These Webpages were found on Social Metric's website at <https://www.socialmetric.com> ("Website"). The Webpages consisted of tables that listed out various particulars of individuals. They were created for internal administrative and client use.

5 The personal data in these nine Webpages included individuals' names; e-mail addresses; contact numbers; employers; occupations; date and time of registration; and other miscellaneous information including, "places to visit" (*eg*, states in Australia), "activities" (outdoor sports) and "purpose" (*eg*, personal growth). In particular, two out of the nine Webpages also contained the personal data (name and age) of about 155 children. The Commissioner's investigations disclosed that such personal data were provided by the individuals directly (*ie*, by the individual sending his or her personal data to Social Metric through Facebook's private message function), and were not obtained from publicly available sources.

6 Based on the date and time of registration of the nine Webpages, it was observed that all the personal data contained therein, except for two individuals, were collected and disclosed before the Personal Data Protection Act 2012[1] ("PDPA") came into full force on 2 July 2014 ("Appointed Day"). In respect of the two individuals, the personal data of one of the individuals (name, e-mail address and contact number) were disclosed on 24 December 2014, while the personal data of the other individual (name and e-mail address) were disclosed on 15 September 2015.

7 Social Metric was first informed by the complainant ("Complainant") of the unintended disclosure of personal data on the nine Webpages on 27 April 2016. Following the complaint made by the Complainant to the Commission, the Commission had also informed Social Metric about the disclosure on the Webpages in May 2016. After being informed about the Webpages, Social Metric took down three out of the nine Webpages.

1 Act 26 of 2012.

However, at the time of the Commissioner's investigation, six out of the nine Webpages were still available on the World Wide Web. These remaining six Webpages contained the personal data of approximately 558 individuals. As at 11 July 2016, all the Webpages had been taken down. The personal data was therefore left on the Webpages for a period of at least two months since the time that Social Metric had first been informed of the personal data that was held on its Website until they were all completely taken down. By the Commissioner's estimate, given that some of the marketing campaigns had ended by the Appointed Day, some of the personal data would have been left on the Webpages for more than two years after the respective events.

## COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

### *Issues for determination*

8 Based on the facts, there were two main issues for determination before the Commissioner:

(a) what Social Metric's obligations were under the PDPA with respect to the personal data found on the Webpages that were exposed on the Internet; and

(b) whether Social Metric had complied with these obligations, specifically:

(i) whether Social Metric had complied with its retention limitation obligation ("Retention Limitation Obligation") under s 25 of the PDPA when it retained the personal data of its clients' customers even after the social media marketing campaigns were over; and

(ii) whether Social Metric had complied with its protection obligation ("Protection Obligation") under s 24 of the PDPA, given the unauthorised disclosure of personal data on the Webpages.

### *Social Metric's obligations under the Personal Data Protection Act*

*How did data protection provisions of the Personal Data Protection Act apply to Social Metric?*

9 As the Webpages were created before the data protection provisions ("Data Protection Provisions") of the PDPA (*ie*, Pts III–VI of the PDPA) came into force on the Appointed Day, it is necessary to examine how Social Metric came to take on these obligations under the PDPA in respect of the Webpages.

10 *Before the Appointed Day*, the Data Protection Provisions of the PDPA were not in force, and hence, Social Metric was not subject to these provisions in relation to the personal data that it had processed for its clients' social marketing campaigns. *After the Appointed Day*, the Data Protection Provisions under the PDPA came into force, and at such time, it became incumbent on an organisation (as in this case, Social Metric) to take proactive steps to comply with these obligations under the PDPA in respect of the *existing* personal data held in their possession or control, as well as any *new* personal data that it may come into possession or control of.

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".

12 What has just been described about the PDPA obligations coming into operation and applying after the Appointed Day is to be contrasted with the "grandfathering" provision under s 19 of the PDPA, which also applies to personal data held by an organisation before the Appointed Day. In essence, s 19 of the PDPA allows an organisation to continue to *use* (but not disclose) personal data that were collected before the Appointed Day for such purposes for which the personal data were collected, without having to obtain consent under the Data Protection Provisions. As mentioned in

*Re Comfort Transportation Pte Ltd*,[2] personal data collected before the Appointed Day as business contact information could continue to be used *after* the Appointed Day as such. Notwithstanding the grandfathering of the purpose for usage, the organisation would have to still comply with the rest of the Data Protection Provisions.

13 From the above analysis, therefore, Social Metric has the obligation to comply with the Data Protection Provisions under the PDPA in respect of the existing personal data that were held on its Website.

*In what capacity did Social Metric take on such obligations under the Personal Data Protection Act?*

14 In order to determine what obligations apply to Social Metric under the PDPA, it is apposite to consider the capacity that Social Metric was in when it was carrying out the data processing activities on the personal data of its clients' customers – *ie*, as a data intermediary or an organisation. This is because different sets of obligations and responsibilities may apply depending on the capacity that Social Metric was in.

15 Under the PDPA, when an organisation carries out data processing activities on behalf of another, the organisation is considered a data intermediary. The PDPA obligations that would apply to a data intermediary pursuant to s 4(2) of the PDPA are limited to two obligations – the Protection Obligation and Retention Limitation Obligation. In comparison, an "organisation" under the PDPA, for which the data intermediary is performing the data processing, would be subject to the full range of obligations under the PDPA. This is so, even though the organisation may have engaged a data intermediary to implement the necessary data protection measures for the organisation. Section 4(3) of the PDPA provides that "an organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself".

2 [2017] PDP Digest 122.

16 Beyond the different sets of obligations that may apply to an organisation or data intermediary, there may also be different responsibilities that an organisation or data intermediary may undertake under the PDPA. As explained in *Re Smiling Orchid (S) Pte Ltd*,[3] in a situation 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 personal data arising from its direct possession of or control over the personal data. This means that the organisation can still be liable for a data breach for failing to meet its responsibility, even though its data intermediary was found to have its own responsibility, and *vice versa*.

17 In this case, at the point of collection of personal data, Social Metric was carrying out the collection on behalf of its clients for the marketing campaigns, and was thus acting as a data intermediary for its clients. Next, with regard to Social Metric posting the personal data of its clients' customers on the Website, that, too, was done in the capacity of a data intermediary. The Website was put up for the purposes of the marketing campaigns of Social Metric's clients. It was when the marketing campaigns had ended, and Social Metric had held on to the personal data (which was still posted on the Website) for a longer period than was *reasonable*, that Social Metric can no longer be considered a data intermediary in relation to such activities.

18 There are two main reasons for this position. First, the social marketing campaigns were already over, and both Social Metric and its clients had no further purpose in retaining the personal data on the Website. Social Metric cannot be said to be "[processing] personal data on behalf of" its clients by the protracted retention of the personal data on its Website. Indeed, as mentioned above, based on the Commissioner's estimate, some of the personal data were kept on its Website for more than two years. Accordingly, at some point in time, Social Metric was no longer a data intermediary within the definition of this term under the PDPA. Instead, Social Metric was now acting on its own accord in relation to the personal data that it held, and had taken on the full responsibility of protecting such personal data. Second, Social Metric had a standard

3 [2017] PDP Digest 133.

operating procedure ("SOP") to dispose of the personal data after the marketing campaigns in its contracts for service with its clients had ended. As far as the clients were concerned, it was reasonable to expect Social Metric to carry out the disposal upon the completion of the marketing campaigns, and there was no evidence that Social Metric's clients were aware that Social Metric had failed to dispose of the personal data. In the premises, it would not be logical nor fair if the PDPA imposes a continuing obligation on Social Metric's clients to protect the personal data. Since Social Metric had failed to carry out what it was supposed to do (*ie*, to dispose of the personal data after the marketing campaigns), it bears the risk for whatever happens to the personal data that were held in its hands after the marketing campaigns were over.

19 Social Metric had therefore assumed the full data protection responsibilities of an "organisation" under the PDPA after the end of the marketing campaigns. This is a position that has been adopted by foreign data protection authorities as well.

*Foreign authorities on the issue of data intermediary taking on responsibilities of organisation*

20 The foreign data protection authorities have taken the position that a data processor, which was originally engaged to perform data processing activities for or on behalf of a data controller, could subsequently take on the data protection responsibilities of a data controller under certain circumstances, for example, where the data processor uses the personal data for its own unauthorised purposes, or for additional purposes not envisaged by the data controller, or for its own benefit.

21 According to the guidance issued by the UK's Information Commissioner's Office, *Data Controllers and Data Processors: What the Difference is and What the Governance Implications are* ("ICO guidance"), a data processor may become a data controller in its own right, albeit to a limited extent, when, for example, the processor breaks the agreement with its data controller. The ICO guidance provides that:[4]

4 UK, Information Commissioner's Office, Data Controllers and Data Processors: What the Difference is and What the Governance Implications are

(*continued on next page*)

> 65. A data processor will have access to the personal data held by the controller or controllers it provides its services to but it cannot have any of its own data controller responsibilities for that data. *However, in certain situations this may change and it will become a data controller in its own right if only to a limited extent.*
>
> …
>
> 67. *If a data processor breaks the agreement with its data controller, for example by using the data for its own unauthorised purposes, then it will also take on its own data controller responsibilities.* This includes the duty under the first data protection principle to process, including to obtain, personal data fairly and lawfully. Where a data processor takes the personal data the controller has entrusted it with but breaks the terms of its contract by using the data for its own purposes, it is likely to be in breach of the first principle and the ICO could take enforcement action against it ….
>
> [emphasis added]

22 Similarly, in the EU, the European Commission has issued *Opinion 1/2010 on the concepts of "controller" and "processor"* which describes a scenario where a data processor which conducts marketing activities may be considered to be a data controller and become subject to data protection obligations:[5]

> In these cases – where there is a good definition of purposes, but little or even no guidance on technical and organizational means – the means should represent a reasonable way of achieving the purpose(s) and the data controller should be fully informed about the means used. *Would a contractor have an influence on the purpose and carry out the processing (also) for its own benefit, for example by using personal data received with a view to generate added-value services, it would be a controller (or possibly a joint controller) for another processing activity and therefore subject to all the obligations of the applicable data protection law.*
>
> Example No. 3: Company referred to as data processor but acting as controller

---

(6 May 2014) <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> at paras 65 and 67.

5 EU, European Commission, Art 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (16 February 2010) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> at p 14.

> Company MarketinZ provides services of promotional advertisement and direct marketing to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for the purpose of promoting products of other customers. *This decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this processing operation.* The question of the lawfulness of this processing will still be assessed in the light of other Articles (6-8).
>
> [emphasis added]

23 This means that where a data processor has an influence on the purpose of the processing, and carries out a separate processing activity which is different from the purpose that the data controller envisaged or which is for the data processor's own benefit, then the data processor could be considered a data controller for that separate processing activity.

24 Whilst Singapore does not have the concept of a "data controller" or a "data processor" in its data protection regime, these terms taken from the UK's Data Protection Act 1998[6] and the EU Directive 95/46/EC do bear similarities to the concept of "organisation" and "data intermediary" respectively in the PDPA. As such, the Commissioner is of the view that the general principles mentioned above are useful and supportive of the position that the Commissioner has taken.

### *Social Metric's compliance with its Retention Limitation and Protection Obligations*

25 Accordingly, while Social Metric had initially held the *de facto* role of a data intermediary (before the Appointed Day) during the marketing campaigns, Social Metric had subsequently taken on the role of an "organisation" when it held on to the personal data on its Website after the marketing campaigns with its clients were over.

26 In this case, the pertinent issues relate to Social Metric's compliance with its Protection and Retention Limitation Obligations. This is because the nature of the breach and the subject of complaint in this case relate to

6 c 29.

(a) Social Metric's failure to protect the personal data on the Webpages from unauthorised access; and (b) Social Metric's failure to remove personal data of its clients' customers from its Website in accordance with its SOP or a reasonable period thereafter justifiable for legal or business purposes ("the tail period"). *These are obligations that are common between Social Metric as data intermediary or as organisation.* Had the period of retention been shorter, and Social Metric stayed as a data intermediary, its alleged misconduct would have been analysed as breaches of the Retention Limitation and Protection Obligations *qua* data intermediary. Where in this case, a considerable period has passed, and the data intermediary has morphed into an organisation, it is not meaningful to split hairs and analyse *part* of the period in which Social Metric had held on to the data as a breach of a data intermediary's Retention Limitation and Protection Obligations while analysing the *rest* of this period as a breach of an organisation's Retention Limitation and Protection Obligations. With the effluxion of time that Social Metric had held on to the data, there was nothing to separate Social Metric's responsibilities under the Retention Limitation and Protection Obligations from that of a data intermediary or an organisation – Social Metric ultimately took on the role and responsibility of an "organisation" under the PDPA for the protection of personal data. The entire period in excess of "the tail period" should be analysed as a breach of an organisation's Retention Limitation and Protection Obligations.

27 We turn now to the assessment of whether or not Social Metric has complied with its Retention Limitation and Protection Obligations.

### *Whether Social Metric has complied with the Retention Limitation Obligation*

28 Under the Retention Limitation Obligation, an organisation is obliged 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: (a) the purpose for which the personal data were collected is no longer served by retaining the data; and (b) retention is no longer necessary for legal or business purposes. As limbs (a) and (b) of s 25 of the PDPA are conjunctive, this means that if the organisation still has purposes for

retaining the personal data under *either* limb (a) or limb (b) of s 25 of the PDPA, the organisation is allowed to retain such personal data.

29 On the facts of this case, Social Metric held on to the personal data even though the marketing campaigns were over. Under limb (a) of s 25 of the PDPA, the purpose for which the personal data were collected was no longer being served by retention of the personal data. Additionally, based on the evidence in this matter, there was nothing to indicate that Social Metric had any legal or business purpose under limb (b) of s 25 of the PDPA for keeping the personal data either. Since the purpose of retention as a data intermediary was no longer valid, retention as an organisation is all the more indefensible. Accordingly, Social Metric has failed to show that it had any purpose for retaining personal data pursuant to limbs (a) and (b) of s 25 of the PDPA, and it is therefore in breach of s 25 of the PDPA.

*Whether Social Metric has complied with the Protection Obligation*

30 As explained at [25]–[26] above, Social Metric has an obligation to protect personal data under the Protection Obligation as an *organisation* under the PDPA (pursuant to s 24 of the PDPA). Social Metric had taken on the role of an "organisation" when it held on to the personal data on its Website after the marketing campaigns with its clients were over, and it was in such a capacity that it had the duty to protect the personal data in its possession or control after the Protection Obligation came into force on the Appointed Day.

31 The Commissioner finds that Social Metric failed to comply with its Protection Obligation. Social Metric had failed to limit access to the Webpages, and had left the personal data on the Webpages exposed to the World Wide Web. There were no security or access controls on the Website or on any of the Webpages, such as a password protection. Any member of the public could have accessed the personal data of the clients' customers through the Webpages.

32 This case is analogous to the case *Re Propnex Realty Pte Ltd*,[7] where it was found that the organisation failed to properly protect personal data as it did not have any security controls or restrictions (*ie*, a proper authentication system) to prevent access from the World Wide Web over the webpages

7 [2017] PDP Digest 171.

that were stored on the server. Similar to *Re Propnex Realty Pte Ltd*, therefore, the present case may be characterised as one in which Social Metric had failed in its Protection Obligation to put in the necessary controls to prevent access to personal data held on its Webpages. It was not one where, for example, the organisation had intentionally disclosed personal data on its website. In those cases, the Commissioner may look into the further issues of whether the organisation was in breach of its consent and notification obligations for disclosing personal data without consent and/or notification. This is illustrated by the case of *Re My Digital Lock Pte Ltd*.[8]

33 Additionally, not only did Social Metric fail to put in the necessary security measures upon the PDPA coming into full force on 2 July 2014 (*ie*, the Appointed Day), this had carried on well after 2 July 2014. As mentioned earlier at [6], there were two instances where Social Metric had uploaded personal data of the two individuals on the Webpages in December 2014 and September 2015 respectively. Social Metric's prolonged failure to put in place the necessary security measures was inexplicable and a flagrant breach of its Protection Obligation under the PDPA.

34 Social Metric alleged that the reason why the customers' personal data were publicly accessible online was due to oversight or forgetfulness on its part. These are not valid excuses.

35 In consideration of the above, Social Metric, in allowing the Webpages containing personal data to be made publicly available and failing to implement reasonable security arrangements over the Webpages, was in breach of the Protection Obligation.

## COMMISSIONER'S DIRECTIONS

36 Pursuant to s 29 of the PDPA, the Commissioner is empowered to give Social Metric such directions as it deems fit to ensure Social Metric's compliance with the PDPA. This may include directing Social Metric to pay a financial penalty of such amount not exceeding $1m as the Commissioner thinks fit.

8 [2017] PDP Digest 146.

37 In assessing the breach and determining the directions to be imposed on Social Metric in this case, the Commissioner took into account the following factors:

(a) the fact that personal data (names and ages) of about 155 children were disclosed;

(b) Social Metric did not take prompt remedial actions after being informed of the data breach by the Commissioner;

(c) Social Metric had, on more than one occasion, informed the Commissioner that the personal data in question had been deleted when this was not the case; and

(d) Social Metric was generally uncooperative throughout the investigation process. Social Metric demonstrated its uncooperative attitude by making unsubstantiated claims such as informing the Commissioner that the data breach was a result of an external hack, and that it had engaged freelance developers located in the Philippines to set up and maintain the Website without providing any evidence of its claims. In addition, Social Metric also caused multiple delays in the investigation process when it repeatedly missed the Commissioner's deadlines to reply.

38 Having completed its investigation and assessment of this matter, the Commissioner is satisfied that Social Metric was in breach of the Protection Obligation and the Retention Limitation Obligation under ss 24 and 25 of the PDPA respectively.

39 In consideration of the relevant facts and circumstances of the present case, the Commissioner hereby directs Social Metric to:

(a) scan and confirm that its Website no longer stores publicly accessible personal data that are not supposed to be disclosed to the public; and

(b) pay a financial penalty of $18,000 within 30 days from the date of the Commissioner's 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.

40 The Commissioner emphasises that he takes a very serious view of any instance of non-compliance with the PDPA, and he urges organisations to

9 Cap 322, R 5, 2014 Rev Ed.

take the necessary action to ensure that they comply with their obligations under the PDPA. The Commissioner will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re Credit Counselling Singapore

## [2018] PDP Digest 295

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-1610-B0261
**Decision Citation**: [2018] PDP Digest 295; [2017] SGPDPC 18

***Personal data*** *– Context of disclosure rendered personal data sensitive – Stronger controls needed to protect sensitive personal data*
***Protection Obligation*** *– Disclosure of personal data – Insufficient administrative security arrangements*

29 December 2017

### BACKGROUND

1 An administrative staff ("admin staff") of Credit Counselling Singapore ("CCS" or "Organisation") had sent out a mass e-mail to 96 individuals of the Organisation's debt management programme ("DMP"), which exposed their e-mail addresses and associated names (for some individuals) to all recipients. The Commissioner found this to be an unauthorised disclosure of personal data, including the identity of individuals who were on the DMP. The Commissioner found the Organisation to be in breach of its protection obligation ("Protection Obligation") under the Personal Data Protection Act 2012[1] ("PDPA"). The Commissioner's findings and grounds for his decision are set out below.

### MATERIAL FACTS

2 The Organisation is a registered charity under the National Council of Social Services. The Organisation provides assistance to debt-distressed individuals (whom it calls "clients"), such as credit counselling and

1 Act 26 of 2012.

facilitating the establishment of a debt-restructuring plan with creditors. The DMP is a voluntary debt repayment scheme under which the Organisation helps clients, who are facing difficulties or unable to repay their unsecured consumer debts, to work out a payment arrangement with their creditors.

3 The data breach occurred when the Organisation sought to obtain a status update from its clients on the debts to be repaid to their creditors under the DMP. At the material time, the Organisation had a total of [redacted] "active" DMP clients, of which 810 clients had received the questionnaire from the Organisation via post requesting for a repayment status update. Of these 810 clients, 297 clients failed to respond by the deadline. The Organisation then sent three batches of follow-up e-mails to these 297 DMP clients.

4 On 30 September 2016, an admin staff of the Organisation made a mistake when sending out one of the three batches of follow-up e-mails ("Follow-up E-mail"). Instead of pasting the e-mail addresses of 96 DMP clients in the "Bcc" field, the admin staff had inadvertently pasted the e-mail addresses in the "To" field before proceeding to send the Follow-up E-mail out. This mistake caused the 96 e-mail addresses and associated names (for some individuals) to be displayed in the "To" field and were thus visible to all the recipients of the Follow-up E-mail.

5 Subsequently, the Organisation received feedback from four DMP clients who were concerned that their identity had been disclosed to the rest of the recipients. In addition, two DMP clients had clicked the "Reply All" button when submitting their completed questionnaire to the Organisation, which resulted in inadvertent disclosure of additional personal data (contained in the questionnaire) to all the other recipients.

## COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

### *Main Issues for Determination*

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

(a) whether the information disclosed by the Follow-up E-mail constituted personal data; and

(b) whether the Organisation had put in place reasonable security arrangements to protect the personal data set in its possession or in its control, as required under s 24 of the PDPA.

### *Issue (a): Whether information disclosed by Follow-up Email constituted personal data*

7 The starting point is whether the Follow-up E-mail that was sent out by the Organisation had disclosed personal data of the 96 DMP clients.

#### *The 96 e-mail addresses were personal data*

8 Section 2(1) of the PDPA defines "personal data" to be data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. In this case, all 96 e-mail addresses disclosed in the Follow-up E-mail are considered personal data under the PDPA because the Organisation would also have the name of the individual to whom the e-mail address belongs to, and would thus be able to identify the individual from that e-mail address. The Protection Obligation therefore attaches to the e-mail addresses both as part of the Organisation's complete records of its DMP clients as well as when used on their own.

9 A copy of the Follow-up E-mail that was provided to the Personal Data Protection Commission ("Commission") revealed that there were three categories of e-mail addresses: (a) an e-mail address which disclosed the full name of the individual, *eg*, "tan.ah.kow980@gmail.com"; (b) an e-mail address which contained the partial name of the individual, *eg*, "ylt.rachel@hotmail.com"; and (c) an e-mail address from which no individual's name could be deciphered, *eg*, "foodlover721@hotmail.com".[2] *Prima facie*, the disclosure of e-mail addresses coming under categories (a) and (b) would allow an outsider to identify the individual because the name or partial name of the individuals have been disclosed. Therefore, even from

2 For the avoidance of doubt, these examples are not the actual e-mail addresses disclosed in the data breach and are purely for illustration purposes only. Any resemblance to an actual e-mail address is purely coincidental, and there is no intention to identify any individual.

the perspective of an outsider, the Follow-up E-mail had disclosed personal data of individuals to the outsider for categories (a) and (b) above.

10 Additionally, investigations revealed that out of the 96 e-mail addresses that were disclosed, 16 individuals could be identified on online social media platforms based on a search of their e-mail addresses. As stated above, the definition of "personal data" under the PDPA includes data that can be identified from (a) that data coupled with (b) other information to which the organisation has or is likely to have access. Since the "other information" that is needed to identify the 16 individuals behind the e-mail addresses disclosed is readily available on various social media platforms, the e-mail addresses of those 16 individuals would allow a person who had access to the e-mail addresses to identify the 16 individuals. In this day and age where access to the Internet is prevalent and there is widespread use of social media platforms, it would be unrealistic to ignore the Internet as a source of information to identify an individual.

*Context of Follow-up E-mail rendered communication content and personal data sensitive*

11 This is a case where the personal data, in the form of contact details, which ordinarily would not have been sensitive, were rendered sensitive by reason of the context of their disclosure. The nature and context of the Follow-up E-mail is crucial to this analysis. As mentioned above, the Organisation had sent the Follow-up E-mail as part of the periodic update from its DMP clients to obtain the status of their debt repayment. The Follow-up E-mail contained a "DMP Status Update Form" in which individuals were required to provide the Organisation with information about their state of indebtedness by selecting one of several available options. For example, one option was "I have completed my DMP repayment to all my creditors … Please assist to remove my DMP status from my Credit Bureau Singapore's credit report". Another available option was "I am servicing my DMP repayment every month with no missed payment in the last 12 months". Yet another option that individuals could select was "I have missed one or more payments in the last 12 months and I wish to seek assistance from CCS. I will contact CCS within the next two weeks to discuss my case". Further down the form, the individual was to fill up his particulars, including his name and NRIC number.

12 Given the above, the fact that an individual is included on the list of e-mail addresses in the Follow-up E-mail would indicate that the individual is either currently facing financial debt, or was previously in debt, and that the individual is obtaining, or had previously obtained, assistance under the DMP scheme to pay off the debt.

13 Therefore, if an individual's identity had been revealed by the disclosure of his or her e-mail address in the Follow-up E-mail, it would also mean that the individual's financial information (*ie*, his debt status as a current or former debt-distressed individual) would be divulged by the Follow-up E-mail.

14 At the time when the Follow-Up E-mail was sent out by the Organisation, it contained a blank DMP Status Update Form, and hence, no other personal information of individuals was disclosed to the recipients of the Follow-Up E-mail beyond the disclosure of the individual's financial information.

15 That the financial information is sensitive personal data of an individual is a position that has been taken by the Commissioner, as well as foreign data protection authorities.

16 In the earlier decisions of the Commission, the Commission found that financial information such as a policyholder's bank account details (consisting of the name of the bank, branch of the bank, the bank account number and the account holder's name);[3] and an individual's central depository account details (consisting of the account holder's name, address, account number, securities holdings, transaction and payment summaries)[4] to be personal data that are of a sensitive nature.

17 The Information and Privacy Commissioner for British Columbia has taken a similar position in a case involving the unauthorised disclosure of the names of the members of trade unions, as well as the amount of strike pay they were paid and still owed to the union. The commissioner took the view that:[5]

---

3 *Re AIA Singapore Private Limited* [2017] PDP Digest 73 at [5] and [19].

4 *Re Central Depository (Pte) Limited* [2017] PDP Digest 81 at [8] and [24].

5 *Order P17-01: Construction Maintenance and Allied Workers Local 2423* <https://www.oipc.bc.ca/orders/2020> at [39].

> *[F]inancial information connected to an individual is generally sensitive information, particularly when it involves a debt.* Owing money to another party (whether an individual or any legal entity) is generally a private matter between those parties. In my view, *the fact that money was borrowed and is owed could, whether justified or not, lead to moral judgements about the individuals and their spending, financial choices, earning power or about their character generally. In particular, a lapse in, or lack of, payment to that party may be considered particularly sensitive information, given the stigma that may be attached to an individual having a delinquent debt.* [emphasis added]

18 In another Canadian case, the Information and Privacy Commissioner of Alberta found that the actions of an employee of an organisation, who had disclosed personal data (comprising an individual's name, telephone number, creditor name, amount owing, last payment amount, last payment date and unique account number) to an unauthorised third-party debt settlement agency, had caused there to be a real risk of significant harm posed to the affected individuals. In finding the organisation in breach of the Personal Information Protection Act ("PIPA"), the commissioner stated that:[6]

> [T]he personal information involved could be used to cause harm to affected individuals *in the form of financial loss, embarrassment and harassment by an unauthorized third party debt collection agency*. In my view, these are significant harms. [emphasis added]

Given the type of sensitive personal data disclosed, the commissioner took the position that this would give an unauthorised debt collection agency "enough personal information to potentially convince affected individuals it is authorized to collect the debt",[7] which would then lead to the abovementioned harms.

19 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.

---

6 *P2015-ND-02: CBV Collection Services Ltd* <https://www.oipc.ab.ca/media/386982/P2015_ND_02.pdf> at p 3.

7 *P2015-ND-02: CBV Collection Services Ltd* <https://www.oipc.ab.ca/media/386982/P2015_ND_02.pdf> at p 3.

20 The above view is captured in the comments provided by the UK Information Commissioner's Office ("ICO") in its *Guide to Data Protection*. When considering the definition of "sensitive personal data" under the UK Data Protection Act 1998,[8] the ICO explained that "[t]he presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data".[9]

21 It is also worth pointing out that the Office of the Privacy Commissioner of Canada ("OPC") has taken the position that "a simple reference to an outstanding debt, even without disclosing specific details about the debt, is personal information".[10] In that case, a bank had telephoned the complainant's employer after a confrontation between the complainant and a bank manager. The employer's internal affairs bureau then sent an internal e-mail which stated that the complainant was involved in a civil dispute with the bank, and that he had "incurred a sizeable debt and was under financial pressure".[11] The commissioner found that this internal e-mail containing that single reference to the complainant's indebtedness and financial situation was personal information that should not have been disclosed.

22 In Hong Kong, the Officer of the Privacy Commissioner for Personal Data ("PCPD") has taken the position that financial information, including an individual's indebtedness, constitutes sensitive data. The PCPD's

8 c 29.

9 UK, Information Commissioner's Office, *Guide to Data Protection*: Key Definitions of the Data Protection Act (7 July 2017) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/> at p 4.

10 See Office of the Privacy Commissioner of Canada, *Interpretation Bulletin: Personal Information* (October 2013) Pt III: Application in Different Contexts <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/#fn41> at fourth bullet point in the "Financial Context" section, p 3.

11 *PIPEDA Case Summary #2003-267: Bank Discloses Customer's Personal Information to Employer* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2004/pipeda-2004-267/> at p 1.

*Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry* provides that:[12]

> *Information showing the financial problems of a customer such as default in payment is commonly recognised as sensitive data, and should therefore be handled with extra care.* Such data should not be disclosed to any third party unless there is a real need to do so. [emphasis added]

The guidance goes on to suggest measures that organisations can take when sending mail to debtors in order to avoid situations where the debtor's personal data is divulged to or accessed by unintended recipients.

23 Accordingly, the personal data that were disclosed in this case was not ordinary personal data but "sensitive" personal data. As will be elaborated on below, 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.

24 Given that the disclosure of e-mail addresses was made by the Organisation inadvertently (as opposed to an *intentional* one), the issue for determination is whether the Organisation had put in place reasonable security arrangements to protect the personal data of its DMP clients against unauthorised disclosures pursuant to s 24 of the PDPA.

### *Issue (b): Whether the Organisation has complied with its Protection Obligation under section 24 of the Personal Data Protection Act*

#### *Stronger controls and greater measures needed to protect sensitive personal data*

25 When it comes to the protection of sensitive personal data, there is a need to put in place stronger security measures because of the actual or potential harm, and the severity of such harm, that may befall an individual from a misuse or unauthorised use of such data. The *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* states that an organisation should "design and organise its arrangements to fit … the possible harm

12 Hong Kong, Officer of the Privacy Commissioner for Personal Data, *Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry* (October 2014) <https://www.pcpd.org.hk/english/resources_centre/industry_specific/files/GN_banking_e.pdf> at para 3.8.2.

that might result from a security breach", and to "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity".[13]

26 Some examples of these precautions to protect sensitive personal data include, but are not limited to, good e-mail procedures and encryption technology. The *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* specifically encourages organisations to undertake security measures to prevent the sending of personal data to the wrong recipients, including "[implementing] email procedures to ensure all emails sent externally to a group of recipients have the recipients' email addresses placed in 'bcc' fields to avoid disclosing recipients' email addresses to all other recipients of the email".[14] In another example, the *Guide to Securing Personal Data in Electronic Medium* suggests organisations adopt encryption as a security measure when e-mails contain confidential or sensitive personal data that "has a higher risk of adversely affecting an individual if such personal data is compromised".[15]

27 In adopting this view on implementing greater safeguards for more sensitive personal data, the Commissioner agrees with the observations made by the OPC in *PIPEDA Report of Findings #2014-003* that organisations "must protect personal information by implementing security safeguards appropriate to the sensitivity of the information" and that the "more sensitive information should be safeguarded by a higher level of protection".[16] In that case, the OPC found that an insurance company had lost its policyholders' files containing sensitive personal data as the

---

13 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the PDPA* (revised on 27 July 2017) at para 17.3.

14 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* (published on 20 January 2017) at para 2.1, ninth bullet point, p 5.

15 Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* (revised on 20 January 2017) at para 14.3.

16 *PIPEDA Report of Findings #2014-003: Insurance Company Overhauls Its Security Safeguards Following Privacy Breach* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-003/>, first and second bullet points in the "Lessons Learned" section at p 2.

safeguards for the control and tracking of the insurance files at the time of the data breach incident were inadequate.

*The Organisation failed to implement adequate administrative security measures*

28 The Organisation's mistake of pasting the list of recipient e-mail addresses in the "To" field instead of the "bcc" field was a straightforward one, and could have been quite easily repeated. All it takes is just a few "wrong" clicks of the button, and the list of e-mail addresses could be pasted in the wrong field and sent out with the unauthorised disclosure of e-mail addresses. Yet the impact of the unauthorised disclosure cannot be ignored – personal information of 96 clients, including their sensitive financial information, had been disclosed with the potential that such disclosure may cause harm to these individuals.

29 It is precisely that the mistake can be so easily *made* and *repeated* which draws into focus the issue with the Organisation's arrangements to protect personal data. The Organisation did not have the appropriate checks and controls to prevent or minimise such mistakes from occurring (which could easily happen again). The types of checks and controls to be implemented could range from an additional layer of supervision or oversight before the e-mail is sent, to sending such e-mails individually (*eg*, using the mail merge function of Outlook). Whatever the way, the staff runs through the important steps to be taken with his or her supervisor, who can provide guidance or corrections to the staff before the action is carried out. Alternatively, it could be in the form of a technical control which ensures that the e-mail addresses are correctly pasted in the "bcc" field of the e-mail instead of the "To" field. The Organisation, however, did not have any checks or controls in place.

30 The Commissioner is not suggesting that organisations would need, for example, to have the added layer of supervision in *all* cases where e-mails containing personal data are being sent out. As mentioned above, organisations are to put in place security arrangements that are commensurate with the sensitivity of the data in question – a balance of considerations. In relation to personal data that is of a *non-sensitive* nature, it may be the case that a second layer of checks is not needed for admin staff to send out the e-mail, if, for example, the admin staff has gone through the relevant training on data protection.

31 However, since the personal data here were of a sensitive nature, the Organisation needed to implement a higher level of security to protect the data (as so described at [25]–[27] above). As mentioned above, the Organisation's lack of any checks and controls was unacceptable in the given context. Moreover, the Organisation did not seem to have taken any steps towards protecting the personal data. This is evident from the lack of differentiation, in the Organisation's processes, between an e-mail that was sent out by the Organisation which *did not* contain personal data, and an e-mail which contained personal data (and sensitive personal data). In both cases, the admin staff was able to send out the e-mail indiscriminately, without requiring further precautions or steps to be taken to protect those e-mails which contained personal data.

32 The nature of the Organisation's work is a relevant factor to be taken into consideration. It routinely handles large volumes of sensitive financial personal data of individuals. This being the case, it is foreseeable that there will be risks of inadvertent disclosure of sensitive personal data. The process in which e-mails containing reminders to submit repayment status updates are sent to its clients ought to have been identified as one which carries with it a significant risk of inadvertent disclosure. There was therefore no excuse for the Organisation not to already have a system of checks and controls in place to prevent or minimise such unauthorised disclosure of personal data. As a matter of good practice, the Organisation could have also carried out a data protection risk assessment, which would have helped to identify and address the specific risk of disclosure that has arisen in this case.

33 The Organisation mentioned that, at that time, it had planned to put in place a "mail-merge" software which would allow for mass e-mails to be sent individually to clients. But it had only started using it from November 2016 onwards; by which time the Follow-up E-mail had already been sent out (it was sent out on 30 September 2016). The fact that there was a solution like the "mail-merge" software which could have ameliorated the risks of unauthorised disclosure of personal data also exemplifies the Commissioner's position that the Organisation could have done more to protect the personal data of its clients. With the benefit of hindsight, perhaps this incident would have been avoided had the mail merge solution been implemented sooner.

34 Given the Commissioner's findings above that the Organisation has not put in place adequate security arrangements to protect the personal data

of its clients, it is therefore concluded that the Organisation was in breach of the Protection Obligation under s 24 of the PDPA.

## COMMISSIONER'S DIRECTIONS

35 In respect of the Commissioner's findings 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 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 $1m as the Commissioner thinks fit.

36 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) information about an individual's adverse financial condition and/or state of indebtedness was sensitive personal data, and the disclosure of which could cause actual or potential harm, injury or hardship to the individual, including serious reputational damage and embarrassment;

(b) given the nature of the Organisation's business of handling large volumes of sensitive personal data, the Organisation ought to have put in place a system of checks for any sensitive personal data that may be disclosed, but it did not do so; and

(c) the data breach incident may cause members of the public to lose trust in such credit counselling organisations to safeguard their personal data, which may frustrate the larger national credit management efforts.

37 The Commissioner also took into account the following mitigating factors:

(a) the Organisation had co-operated fully with the Commissioner's investigations and had readily admitted its mistake without delay;

(b) the Organisation had promptly notified all the affected recipients of the data breach incident and offered them an apology alongside a request to delete the Follow-up E-mail;

(c) the Organisation has counselled the admin staff who made the mistake, and has taken further steps to prevent future data breaches such as its plans to conduct an organisation-wide refresher course on

compliance with the PDPA, and deploying the "mail-merge" software, mentioned above, within two months; and

(d) there were no other data breach incidents reported apart from this one.

38 Having carefully considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of $10,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court[17] in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

17 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

## Re ComGateway (S) Pte Ltd

## [2018] PDP Digest 308

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-1611-B0368
**Decision Citation**: [2018] PDP Digest 308; [2017] SGPDPC 19

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

29 December 2017

### BACKGROUND

1 On 29 November 2016, the complainant ("Complainant"), a customer of the organisation ("Organisation"), informed the Personal Data Protection Commission ("Commission") that:

(a) when the Organisation provided a shipping details webpage ("Shipping Webpage"), it disclosed the Complainant's personal data (in the form of shipping details) to another customer ("First Data Breach"); and

(b) the uniform resource locator[1] ("URL") of the Shipping Webpage of one customer could be manipulated to enable access to shipping details of other customers, by changing the last character ("Second Data Breach").

2 The shipping details included personal data such as the customer's name, contact number and address.

1 www.comgateway.com/ship_track_detail?shipId=MTYwMTExMQ.

3 The Commissioner ultimately found the Organisation not to be in breach of the Personal Data Protection Act 2012[2] ("PDPA") in respect of the First Data Breach, but in breach of s 24 of the PDPA in respect of the Second Data Breach. The Commissioner's findings are now set out below.

## MATERIAL FACTS

4 The Organisation operates an online portal that provides logistics, shopping ("buy-for-me") and shipping services to its customers.

5 The Organisation uses an electronic system and application through and on its website ("Website") to process, track and manage shipping/transaction orders from its customers.

6 The Organisation had been conducting quarterly "Trustwave" vulnerability scans and annual penetration tests for its external and internal networks. The vulnerability scans were used to identify and report on network security vulnerabilities that could be exploited by cybercriminals. The internal penetration test was conducted to evaluate the resiliency of the Organisation's systems to various attacks launched against internal network resources from the perspective of an unauthenticated attack on the internal network. The external penetration test was conducted to evaluate the resiliency of the Organisation's systems and networks to various attacks launched from the Internet. The Organisation had also signed up for a managed firewall application which monitors and protects its networks against attacks and data loss.

7 Additionally, as part of its overall information technology ("IT") security arrangement, the Organisation also ran automated code checks to detect any "OWASP" top ten application security risks on its Website. The Organisation had last passed all the mentioned scans and tests in 2016 before the occurrence of the First and Second Data Breaches.

2 Act 26 of 2012.

***First Data Breach***

8 On 28 November 2016, the Complainant was informed by another customer of the Organisation that when she accessed the Shipping Webpage, it displayed the Complainant's name, contact number, address and shipping details.

9 This was the first time that such an error had been reported to the Organisation; further, the Organisation was unable to reproduce the error. It had subsequently conducted tests and investigations to determine the cause of the First Data Breach, but was unable to determine conclusively the root cause because:

(a) tests conducted on the components of the Website responsible for generating unique shipment IDs ("Shipment IDs") confirmed that these components were functioning properly and that each shipment/transaction record had been assigned a unique identifier;

(b) a review of the code used on the Website did not uncover any coding issues or deficiencies that could have caused the breach;

(c) there were no known session variable management issues associated with the Apache Tomcat software that the Organisation was using;

(d) a review and analysis of log files relating to the First Data Breach revealed that there was no session corruption that could have caused the breach; and

(e) attempts to reproduce or replicate the breach in the production environment of the Website, *eg*, by generating multiple transactions in the same minute, were not successful.

10 Even though the root cause of the First Data Breach could not be determined, the Organisation has since taken the following remediation steps:

(a) removing all personal data from the Shipping Webpage such that even if the wrong Shipping Webpage was sent to a customer, no personal data will be included in the shipping details; and

(b) implementing a logging function that creates a log entry whenever a session variable mismatch occurred, which would provide the Organisation with diagnostic data.

### *Second Data Breach*

11 The complaint relating to the Second Data Breach is of a different nature. Unlike the First Data Breach, the Second Data Breach concerns the Shipping Webpage and how its URL could be manipulated to enable access to the shipping and personal details of the Organisation's customers. The URL for the Shipping Webpage is sent by e-mail to the Organisation's customers.

12 Each of these URLs would take the following form: *eg*, <www.comgateway.com/ship_track_detail?shipId=MTYwMTExMQ>, which comprises the host information (*ie*, www.comgateway.com), the path information (*ie*, ship_track_detail?), and most importantly a unique query string that is associated with the particular shipment to which the URL concerns (*ie*, shipId=MTYwMTExMQ).

13 The Website allocates a unique Shipment ID for each shipment. The unique query string of the URL for the Shipping Webpage is formed by encoding the Shipment ID in Base64 (a binary to text encoding scheme). In the example above, the query string "MTYwMTExMQ" is encoded from the Shipment ID "1601111".

14 As will be explained below, this format of URL string made it possible for anyone to gain access to a customer's Shipping Webpage by taking a URL and systematically changing the last character of the URL until, through trial and error, a workable link is derived.

15 After receiving notice of the complaint, the Organisation has since addressed this vulnerability by adding another unique variable to the URL of the Shipping Webpage to prevent manipulation.

## FINDINGS AND BASIS FOR DETERMINATION

### *Issues to be determined*

16 The shipping details that were compromised had comprised of names, contact numbers and addresses of individuals. These were "personal data" as defined under the PDPA.

17 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.

18 The issues in the present case are:

(a) in respect of the First Data Breach, whether the Organisation had breached s 24 of the PDPA when the Complainant's personal data were rendered accessible to another customer of the Organisation in the manner described at [8] above; and

(b) in respect of the Second Data Breach, whether the Organisation had breached s 24 of the PDPA when personal data of other customers of the Organisation were rendered vulnerable and accessible through the manipulation of the URL of the Shipping Webpage in the manner described at [11]–[14] above.

### *First Data Breach*

19 The fact that personal data had been rendered accessible 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 make reasonable security arrangements to protect personal data.

20 In *Re Singapore Telecommunications Limited*,[3] even though a coding issue in the database script of Singapore Telecommunications Limited's ("SingTel") ONEPASS electronic service had caused an individual's personal data to be revealed to other customers of SingTel, the Commissioner found that SingTel was not in breach of s 24 of the PDPA because SingTel had put in place reasonable security arrangements to protect personal data, including:

(a) a contract requiring its IT service provider, Tech Mahindra, to comply with the PDPA and SingTel's access and security policies;

(b) operational procedures and checks to ensure that its service provider had carried out its functions to protect personal data; and

(c) conducting annual on-site security reviews and penetration tests as part of its governance process.

3 [2018] PDP Digest 148.

21 The position taken by the Commissioner in SingTel is also consistent with that taken by data protection authorities in other parts of the world:

(a) In *PIPEDA Report of Findings #2014-004*,[4] the Office of the Privacy Commissioner of Canada ("OPC") found that an organisation had appropriate safeguards in place to protect personal information at the time of a data breach, even where an individual's personal information could have been accessed by a cyber-attacker. This finding was made after the OPC determined that the organisation had numerous technical safeguards in place at the time of the data breach aimed at preventing and detecting breaches, including (i) the use of firewalls; (ii) encryption of sensitive information; (iii) separate storage and obfuscation of encryption keys; and (iv) multiple intrusion detection systems (through which the breach was detected). The effectiveness of these safeguards was also independently evaluated on a regular basis through external vulnerability scans and audits.

(b) In *Sony PlayStation Network/Qriocity: Own Motion Investigation Report*,[5] the Office of the Australian Information Commissioner ("OAIC") investigated Sony Computer Entertainment Australia Pty Ltd and its related companies ("Sony") following reports of unauthorised access to personal information of Sony's customers on the Sony PlayStation/Qriocity Network. Upon investigation, the OAIC determined that Sony had taken reasonable steps to protect information on its network at the time of the data breach because Sony had a range of security safeguards in place to protect the personal information held, including (i) physical, network and communication security measures to protect the information collected and stored in the network; (ii) encryption of credit card information; and (iii) internal IT security standards that are based on the ISO standards for international information security.

---

4 *PIPEDA Report of Findings #2014-004: Online Service Provider That Suffered a Breach Had Appropriate Safeguards in Place* (23 April 2014) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-004/>.

5 *Sony PlayStation Network/Qriocity: Own Motion Investigation Report* (29 September 2011) <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity>.

22 In the present case and in relation to the First Data Breach, the fact that the cause of the data breach could not be established or that it was possibly a rare computer glitch did not absolve the Organisation of liability under s 24 of the PDPA. The Organisation must show that it had taken reasonable steps to protect personal data held in its possession and/or control. In this regard, the Commissioner is satisfied that the Organisation had, indeed, made reasonable security arrangements to protect personal data from unauthorised access. By virtue of the Organisation's IT system undergoing regular and rigorous IT security tests and scans on the system as described at [6] and [7] above, and that the IT system had successfully passed all those tests and scans, this was a sufficient indication that the Organisation's IT security measures in place were adequate. Additionally, in respect of the First Data Breach, there was no evidence of any issues with the Website functions or services, which would affect the protection of the personal data held on the Website. This case appears to have given rise to an anomalous data breach that could not be replicated.

23 Accordingly, the Commissioner finds that the Organisation has not contravened s 24 of the PDPA in relation to the First Data Breach.

24 As mentioned above, the Organisation has since removed all personal data from its Shipping Webpages, such that even if the same glitch were to recur, there would not be unauthorised access to personal data. While it is the prerogative of the Organisation to take such steps, the Commissioner does not advocate the removal of personal data purely as a risk avoidance measure if the removal detracts from the usability of the Organisation's Website. Such steps would in the Commissioner's view be excessive and unnecessary, especially if there are other reasonable technical or operational means to achieve the objective of protecting personal data.

### *Second Data Breach*

25 In relation to the Second Data Breach, the Commissioner had found that the URL of the Organisation's Shipping Webpages was susceptible to manipulation.

26 From 2 July 2014 (the appointed day when the data protection obligations of the PDPA came into effect) until the Organisation instituted the measures described at [15] above, about 108,085 customers had made shipments via the Organisation. In this regard, the personal data of those

customers (contained in the Shipping Webpages) were vulnerable to unauthorised access and their security could have been compromised.

27 As mentioned at [13] above, the URL of the Shipping Webpage is unique to each customer by virtue of a unique identifier (*ie*, the Shipment ID encoded in Base64) at the end of the URL string. While seemingly a random string of letters (in upper/lowercase), encoding a Shipment ID using Base64 is not an actual means of encryption. Base64 is a common and simple encoding scheme for ensuring that only basic and printable characters are used, and to avoid reserved characters which may have special meanings. Simply put, Base64 is a means of translating the Shipment ID of "1601111" from Arabic numerals, to another language more suitable for use in URLs. Any item encoded in Base64 can be easily decoded through publicly available decoding tools.

28 A person with IT knowledge would be able to recognise that the Shipment ID in the query string was encoded in Base64. Upon decoding the query string, it would also be readily observable or deducible that the Shipment ID is simply a function of the date of shipment and its sequence. With this information, one could reverse engineer and generate valid URLs of the Shipping Webpages of the Organisation's customers or even run a script to harvest personal data from such Shipping Webpages. Even an ordinary user could systematically replace the last character of the URL of a provided Shipping Webpage to arrive at valid URLs of Shipping Webpages of the Organisation's customers, which could then be accessed for the shipping details and personal data of those customers.

29 A test conducted on the query string showed that the URL of the Shipping Webpage could be easily manipulated to obtain a valid URL of the Shipping Webpage of another Shipment ID.[6] During the test, it was discovered that by sequentially replacing the last character of the encoded Shipment ID from A–Z (including both capital and small letters) and 0–9, it was possible to derive three other valid URLs.

---

6 The vulnerable URL portion, *eg*, MTYwMTExMQ, when decoded, is 1601111. This string of numbers consists of the date (yy/mm/dd) and the sequence of the shipment for that date. By changing the last character to small letter "a" to "f", the decoded results are 1601111; changing to "g" to "v" yielded 1601112; and changing to "w" to "z" resulted in 1601113.

30 The Organisation also did not place limits or restrict access to the URLs so that only a specific customer of the Organisation has access to his own shipping details. Anyone could access the URL of a Shipping Webpage and the personal data contained therein without needing to authenticate or to furnish information to verify the identity of the person that was accessing the URL. This allowed for another customer or even an outsider to have access to the customer's shipping details.

31 The personal data held on the Shipping Webpage were, therefore, not secured from unauthorised access online. The ease of manipulation of the URL of the Shipping Webpage to derive the URL of other Shipping Webpages, and the absence of any other security or access-control measures to protect the Shipping Webpages, taken together, meant that personal data on the Shipping Webpages could be easily accessed by any person. Such a person could gain access to the personal data held on the Shipping Webpages, whether or not the person was a "motivated intruder" who had sought to gain unauthorised access to personal data of other individuals, or a person who had accidentally typed in an incorrect query string into the URL address bar.

32 In the response provided by the Organisation, the Organisation admits that at the time of design and implementation of the Website and Shipping Webpage, they had not considered the susceptibility of the Shipping Webpage URL to manipulation and had, therefore, not taken any step to test or address this vulnerability.

33 Given the absence of any security arrangements to protect personal data against such unauthorised access, the Commissioner finds that the Organisation has contravened s 24 of the PDPA in relation to the Second Data Breach.

34 Although the Organisation had in place security arrangements (described at [6] and [7] above) to protect personal data on its Website, including regular vulnerability scans, penetration tests, risk assessments and automated code reviews, none of these arrangements, as the Organisation admits, addresses the URL manipulation vulnerability. Hence, they would not assist the Organisation in avoiding liability under s 24 of the PDPA in respect of the Second Data Breach.

35 This is not the first case where the Commissioner has found a failure to make reasonable security arrangements to protect URLs from being easily

manipulated to compromise the security of personal data, to be a contravention of Section 24 of the PDPA:

(a) In *Re Fu Kwee Kitchen Catering Services*,[7] the URL of Fu Kwee Kitchen Catering Services' ("Fu Kwee") webpage for previewing orders could be manipulated easily (by changing the characters at the end of the URL) to retrieve other orders of Fu Kwee's customers containing the customers' personal data. The Commission found Fu Kwee in breach of s 24 of the PDPA for failing to implement reasonable security arrangements to protect personal data.

(b) In *Re Smiling Orchid (S) Pte Ltd*,[8] the URL of Smiling Orchid (S) Pte Ltd's ("Smiling Orchid") webpage for previewing orders could be manipulated easily (by changing the characters at the end of the URL) to retrieve other orders of Smiling Orchid's customers containing the customers' personal data. The Commission found Smiling Orchid in breach of s 24 of the PDPA for failing to implement reasonable security arrangements to protect personal data.

## DIRECTIONS

36 Given the Commissioner's findings that the Organisation is in breach of its obligations under s 24 of the PDPA in respect of the Second Data Breach, 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 $1m.

37 In assessing the breach and determining the directions (if any) to be made, the Commissioner considered the following factors:

(a) the Organisation handles a substantial volume of shipping transactions for individual customers in Singapore and hence a substantial amount of personal data. It is therefore imperative that security arrangements be implemented to protect the personal data of its customers;

7 [2017] PDP Digest 97.

8 [2017] PDP Digest 133.

(b) the Organisation had co-operated fully with the Commissioner's investigations, including undertaking technical and security testing to determine the cause of the breaches;

(c) the Organisation took prompt action (described at [15] above) to remedy the breach when notified by the Commissioner; and

(d) the Organisation had been conducting regular penetration tests, vulnerability tests and code reviews to guard against online security threats.

38 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 $10,000 within 30 days of the Commissioner's direction.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

**Re Sharon Assya Qadriyah Tang**

**[2018] PDP Digest 319**

**Coram**: Tan Kiat How, Commissioner
**Case Number**: DP-1701-B0485
**Decision Citation**: [2018] PDP Digest 319; [2018] SGPDPC 1

***Consent Obligation*** *– Individual engaged in unauthorised selling of personal data*
***Continued disclosure of personal data collected before appointed day***
***Notification Obligation*** *– Individual engaged in unauthorised selling of personal data*
***Personal or domestic capacity***

11 January 2018

## BACKGROUND

1 This is the first reported case of an individual ("Respondent") who was involved in the unauthorised selling of personal data. The facts disclose a straightforward breach of the Personal Data Protection Act 2012[1] ("PDPA"), and the Respondent does not deny committing the infringing acts. The Commissioner has accordingly found the Respondent in breach of ss 13 and 20 of the PDPA.

2 The Commissioner's findings and grounds of decision are set out below.

## MATERIAL FACTS

3 The Respondent was employed as a telemarketer from 2004 to 2014. Sometime in 2012, the Respondent started purchasing "leads" to expand the reach of her marketing in order to hit her sales targets. These "leads"

1 Act 26 of 2012.

typically comprised an individual's name, NRIC number, mobile number and annual income range. A lead would typically cost between $0.20 and $0.30.

4 The Respondent bought the leads from unknown online sellers and did not retain the details of these transactions. Also, the Respondent did not check or verify with the sellers that the leads she purchased were obtained legitimately with the individuals' consent.

5 On average, the Respondent would buy approximately 10,000 leads per year. According to the Respondent, her first purchase of leads was sometime in late 2012 and her last purchase was sometime in either May or June 2014. At the material time, the Respondent had in her possession approximately 30,990 leads. The leads were stored in Microsoft Excel spreadsheets.

6 From late 2012 up until 23 February 2017, the Respondent estimated that she had resold the leads she had bought about nine to ten times, typically charging customers between $0.05 to $0.20 per lead, depending on the number they purchased. The Respondent would advertise the sale of the leads on various websites, and customers who wished to buy the leads would make payment to the Respondent via a bank transfer. While conducting these transactions, the Respondent concealed her true identity by using an alias (with a corresponding e-mail address), her husband's bank account number, and a mobile phone number registered under her friend's name. The Respondent estimated she had made a profit of $5,000 from selling these leads. The Respondent explained that she had decided to resell the leads as a sideline to supplement her income. During this period of time, the Respondent was concurrently holding a job as a telemarketer and engaging in an apparel business.

## FINDINGS AND BASIS FOR DETERMINATION

7 The following two main issues were canvassed from the facts for the Commissioner's determination:

(a) whether the Respondent was an "organisation" subject to the data protection provisions ("Data Protection Provisions") of the PDPA; and

(b) whether the Respondent's sale and purchase of leads complied with the consent and notification obligations ("Consent and Notification Obligations") under the PDPA.

8 As a preliminary point, it was not disputed that the 30,990 leads in the Respondent's possession, each of which comprised an individual's name, NRIC number, mobile number and annual income range, fell 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.

### *Whether Respondent was an "organisation" subject to Data Protection Provisions of the Personal Data Protection Act*

9 The Commissioner first determined whether the Respondent was acting as an "organisation" for the purposes of the PDPA. This is a pertinent issue in this case, because the Respondent is an individual, and the Data Protection Provisions[2] are only applicable to an "organisation" under the PDPA. Although the PDPA defines "organisation" broadly to include individuals,[3] an individual is expressly excluded from the Data Protection Provisions in the PDPA if the individual was acting in a personal or domestic capacity.[4] Therefore, when it comes to the application of the PDPA to individuals, it is usually germane to the issue to determine whether the individual was acting in a personal or domestic capacity. If the individual was not acting in a personal or domestic capacity, then she will be treated as an "organisation" for the purposes of the PDPA, and obliged to comply with the Data Protection Provisions.

10 On the facts, the Respondent was clearly not acting in a personal or domestic capacity in respect of the buying and selling of leads. The purchase and sales of the leads were not for her own personal use or purposes, but in order to make a profit. Under the PDPA, "business" includes an activity of any organisation, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his personal or domestic capacity. In this regard, the converse of a person acting in a personal or

2 As borne out by Pts III–VI of the Personal Data Protection Act 2012 (Act 26 of 2012).

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

4 Under s 4(1)(*a*) of the Personal Data Protection Act 2012 (Act 26 of 2012).

domestic capacity is one that acts in a business capacity. This was the case for the Respondent in respect of the purchase and sale of leads.

11 In earlier cases, the Commissioner had also found individuals, namely, a registered salesperson[5] and a financial consultant,[6] to come within the definition of an "organisation" under the PDPA. In those cases, the individuals had been carrying out data processing activities for work or business purposes, and were thus not acting in a personal or domestic capacity.

12 Given the above, the Respondent is an "organisation" for the purposes of the PDPA, and subject to the Data Protection Provisions.

### *Whether Respondent's sale and purchase of leads complied with Consent and Notification Obligations under the Personal Data Protection Act*

#### *Respondent's buying and selling of leads were activities that fell under scope of the Personal Data Protection Act*

13 The PDPA governs the collection, use and disclosure of personal data by organisations. Given that the leads which the Respondent had purchased or sold comprised of personal data of individuals, these were activities that fell under the scope of the PDPA. In respect of the purchase of leads by the Respondent, in which the Respondent *acquired* personal data from the seller of the transaction, this amounted to a "collection" of personal data under the PDPA by the Respondent. In respect of the sale of leads by the Respondent, in which the Respondent *provided* personal data to the buyer of the transaction, this amounted to a "disclosure" of personal data under the PDPA by the Respondent.

14 The relevant obligations under the PDPA that apply to the facts of this case are the Consent and Notification Obligations. The Notification Obligation requires an organisation to inform individuals of the purposes for the collection, use and disclosure of personal data, while the Consent Obligation requires the organisation to obtain consent from the individual for such purposes of the collection, use and disclosure. The appropriate

5 *Re Chua Yong Boon Justin* [2017] PDP Digest 91.

6 *Re Ang Rui Song* [2018] PDP Digest 236.

provisions of the Notification and Consent Obligations are found in the Data Protection Provisions of the PDPA at ss 13 to 15 and 20 respectively.

*Respondent was not subject to Data Protection Provisions in respect of purchase and sale of personal data before Appointed Day*

15 According to the Respondent, she was first involved in the buying and selling of leads since 2012 to support her work as a telemarketer.

16 However, the Data Protection Provisions of the PDPA only came into effect on 2 July 2014 ("Appointed Day"). This means that during the period before the Appointed Day, the Respondent was not subject to or required to comply with the Data Protection Provisions of the PDPA in respect of the collection, use and disclosure of the personal data found in the database of leads.

17 Notwithstanding, after the Appointed Day when the Data Protection Provisions came into force, the Respondent was subject to the obligations under the Data Protection Provisions in respect of both the *existing* personal data held in the Respondent's possession or control, and any *new* personal data that the Respondent may come into possession or control of. The Respondent was therefore obliged to take steps to comply with the Data Protection Provisions in respect of both these sets of data. This includes obtaining consent from the individuals for the use of the personal data for a new purpose, which the individuals had previously not consented to, as it falls outside the purposes for which the personal data was originally collected under s 19 of the PDPA (as will be elaborated on below).

18 This was a position that was taken in *Re Social Metric Pte Ltd*.[7] In that case, Social Metric had processed personal data for its clients' social marketing campaigns all the way back before the Appointed Day. The Commissioner took the position that before the Appointed Day, Social Metric was not required to put in place reasonable security arrangements under s 24 of the PDPA to protect the personal data in its possession or under its control. However, when the Data Protection Provisions came into force after the Appointed Day, Social Metric needed to put in place such security arrangements to protect both the existing and new personal data.

7 [2018] PDP Digest 281.

*Grandfathering provision may apply to continued use but not sale of personal data*

19 As the Respondent had been purchasing and selling personal data since 2012, and before the Appointed Day, the question is whether the Respondent can rely on the "grandfathering" provision under s 19 of the PDPA to continue to *use* or *sell* (*ie*, disclose) such personal data to third parties after the Appointed Day. It should be noted that the Respondent cannot continue to *purchase* or collect personal data after the Appointed Day, as the Data Protection Provisions would have kicked in on the Appointed Day, and would require the Respondent to provide notification to, and obtain consent from, the individuals pursuant to the Consent and Notification Obligations (unless an exception applies).

20 The grandfathering provision provides that organisations may continue to *use* personal data that they have collected before the Appointed Day, for the purposes for which the personal data were collected, unless consent is withdrawn or the individual gives an indication that there is no such consent.

21 In respect of the personal data that were purchased or obtained before the Appointed Day, it may be possible for an organisation to continue using the personal data if such use falls within the purposes of collection, such as for its own reasonable use (*ie*, telemarketing purposes), provided that there was no indication that the individual did not consent to the continued use. This is the position that the Personal Data Protection Commission ("PDPC") articulated in its *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* ("Advisory Guidelines"), of which an extract of the relevant parts is set out below:[8]

> The effect of section 19 is that organisations can continue to use personal data collected before the appointed day for the same purposes for which the personal data was collected without obtaining fresh consent, unless the individual has withdrawn consent (whether before on, or after the appointed day). Organisations should note that section 19 only applies to 'reasonable existing uses' of personal data collected before the appointed day.

8 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at paras 23.3–23.4.

> For the avoidance of doubt, the purpose of telemarketing (i.e. sending a specified message to a Singapore telephone number) could be a reasonable existing use.

22 However, in this case, the Respondent went beyond using the personal data for her own telemarketing purposes, and proceeded to sell personal data to third parties. The "grandfathering" provision only permits the continued "use" of personal data for the purposes for which the personal data were collected. Such "use" does not extend to "disclosure" of personal data unless, as set out at para 23.1 of the Advisory Guidelines, the disclosure "is necessarily part of the organisation's use of such personal data". In the case of the sale of personal data, the disclosure of personal data is the main activity being carried out, and is not incidental to any of the organisation's own uses of the personal data. Thus, it is not a disclosure "that is necessarily part of the organisation's use of such personal data". The PDPC has stated this position in its Advisory Guidelines as an example:[9]

> Organisation XYZ has been selling databases containing personal data. *This would be considered a disclosure of personal data and not a reasonable existing use under section 19*. After the appointed day, XYZ needs to ensure that consent has been obtained before selling these databases again. [emphasis added]

23 Consequently, the grandfathering provision would not apply to the instances where the Respondent had been selling personal data before the Appointed Day, and continued to sell personal data after the Appointed Day. In respect of personal data that were not sold before the Appointed Day, it is all the more so that the Respondent cannot rely on the grandfathering provision, because there was never an existing practice of selling the personal data in the first place, and hence there is no "use" to be carried on in respect of the personal data.

### *Respondent's sale of leads comprising of personal data after Appointed Day was serious contravention of PDPA*

24 During the investigations, the Commissioner found no evidence that the Respondent had continued to purchase leads from the online sources after the Appointed Day. However, there was clear evidence that the

9 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at para 23.6.

Respondent was still selling leads after the Appointed Day. In respect of the Respondent's sale of such leads, the Commissioner finds that there was a clear breach of the Consent and Notification Obligations under the PDPA.

25 When questioned about the sale of personal data, the Respondent admitted that she did not obtain consent from the individuals for the sale of their personal data to third parties. The Respondent also admitted that she did not check or verify with the online sellers if they had obtained consent from the individuals to the selling of their personal data. Similarly, the Respondent had also admitted that she did not provide any notification to the individuals of the sale of their personal data. The Commissioner also carried out further investigations and separately contacted several individuals whose personal data were found in the database of leads, and all of them confirmed that they had not consented to their personal data being disclosed or sold.

26 Accordingly, on the evidence that the individuals had not been informed of the sale of their personal data nor did they provide consent to the sale of their personal data, the Respondent is in breach of both the Consent and Notification Obligations under the PDPA.

27 The sale of personal data in contravention of the PDPA is a serious breach of the PDPA. In the UK, data selling is expressly prohibited by legislation. Section 55 of the Data Protection Act 1998[10] ("DPA") provides that it is an offence for any person who (a) knowingly or recklessly, without the consent of the data controller, obtains or discloses personal data or procures such disclosure, or (b) sells or offers to sell the personal data so obtained. Specifically, s 55(6) of the DPA clarifies that "an advertisement indicating that personal data are or may be for sale is an offer to sell the personal data". In this regard, both the advertisement of the sale of personal data, and the actual sale of personal data carried out, would constitute an offence under the DPA.

28 The UK's Information Commissioner's Office ("ICO") has recently found a data broker to be in breach of the DPA for obtaining customer data from various sources and selling the data to third-party organisations for the purposes of direct marketing. The individuals whose data were traded by the data broker were not informed that their personal data would be

10 c 29.

disclosed to the data broker, or the organisations to which the data broker sold the data on to, for the purpose of sending direct marketing text messages. In total, the ICO found that there were 580,302 records containing personal data that were disclosed without the data subjects' knowledge or consent.[11] In terms of the harm, the ICO stated that "the unlawful trade in personal data [led] directly to the wholescale sending of unsolicited direct marketing texts and the making of nuisance calls", and was satisfied that the "cumulative amount of distress suffered by the large numbers of individuals affected, coupled with the distress suffered by some individuals, means that overall the level was substantial".[12] As such, the data broker was found to be in breach of the DPA and was issued a monetary penalty of £20,000.

29 In Hong Kong, the Office of the Privacy Commissioner for Personal Data ("PCPD") found that the Octopus group of companies ("Octopus Group"), which provides an extensive smartcard payment system for transport and other services, had contravened the requirements of the Personal Data (Privacy) Ordinance[13] by entering into contracts with several business partners to sell its members' personal data without their consent.[14] In that case, the Octopus Group had failed to inform individuals registering for its rewards programme that one of the purposes was the sale of their personal data for monetary gain. This purpose was neither expressly stated in the terms and conditions on the member's registration form, nor could it be said to be a purpose of use within the reasonable expectation of the

11 UK Information Commissioner's Office, *Monetary Penalty Notice: The Data Supply Company Ltd* (27 January 2017) <https://ico.org.uk/action-weve-taken/enforcement/the-data-supply-company-ltd/> at paras 26 and 29.

12 UK Information Commissioner's Office, *Monetary Penalty Notice: The Data Supply Company Ltd* (27 January 2017) <https://ico.org.uk/action-weve-taken/enforcement/the-data-supply-company-ltd/> at paras 32–34.

13 Cap 486.

14 Hong Kong Office of the Privacy Commissioner for Personal Data, *The Collection and Use of Personal Data of Members under the Octopus Rewards Programme Run by Octopus Rewards Limited* (Report No R10-9866) <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R10_9866_e.pdf>.

individuals.[15] In this regard, despite providing their signature on the registration form, the individuals could not be said to have consented to the data selling. It should be noted that the Hong Kong case had a widespread impact, eventually becoming the catalyst for amendments to the data protection law in Hong Kong.

30 The Commissioner likewise takes a serious view of such breaches under the PDPA. There are strong policy reasons for taking a hard stance against the unauthorised sale of personal data. Amongst these policy reasons are the need to protect the interests of the individual and safeguard against any harm to the individual, such as identity theft or nuisance calls. Additionally, there is a need to prevent abuse by organisations in profiting from the sale of the individual's personal data at the individual's expense. It is indeed such cases of potential misuse or abuse by organisations of the individual's personal data which the PDPA seeks to safeguard against.[16] In this regard, the Commissioner is prepared to take such stern action against organisations for the unauthorised sale of personal data.

## ENFORCEMENT ACTION

31 Given that the Commissioner has found the Respondent to be in breach of ss 13 and 20 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Respondent such directions as it deems fit to ensure the Respondent's compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding S$1m as the Commissioner thinks fit.

32 In assessing the breach and determining the directions to be imposed on the Respondent, the Commissioner took into account the following aggravating factors:

---

15 Hong Kong Office of the Privacy Commissioner for Personal Data, *The Collection and Use of Personal Data of Members under the Octopus Rewards Programme Run by Octopus Rewards Limited* (Report No R10-9866) <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R10_9866_e.pdf> at paras 3.36 and 3.40.

16 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim) at p 1: "The personal data protection law will safeguard individuals' personal data against misuse by regulating the proper management of personal data."

(a) the database of leads included personal data of a sensitive nature, *ie*, NRIC numbers and salary ranges of individuals;

(b) the Respondent had used means to obscure her identity when she was selling the leads, which is indicative of a guilty conscience and of a premeditated and deliberate contravention of the PDPA; and

(c) as elaborated above at [30], the profiteering from the sales of personal data by organisations at the expense of consumer or individuals is the very kind of activity which the PDPA seeks to curb, and hence, must be severely dealt with.

33 In relation to the mitigating factors of this case, the Commissioner took into account the fact that the Respondent had candidly admitted to the wrongdoing at the first instance, and co-operated fully with investigations. Additionally, the Respondent was fully co-operative with the Commissioner's investigations and was helpful in providing evidence of the matter.

34 Crucially, the Commissioner also considered the special financial circumstances of the Respondent in determining a suitable amount of financial penalty to impose on the Respondent. During the course of investigation, the Commissioner learnt that the Respondent and her husband were of limited financial means and were earning modest salaries, and had a child and family to support. In the Commissioner's assessment, imposing a high financial penalty on the Respondent would likely place a crushing burden on the Respondent and her family in the circumstances and cause undue hardship.

35 From the evidence, the cumulative amount of payment received by the Respondent from the sale of the leads was unlikely to exceed $5,000, and this was based on a conservative estimate. In addition, the investigation showed that the Respondent was not carrying out the sale and purchase of personal data on a large-scale basis, but was simply conducting these activities opportunistically and on the side to supplement her income.

36 Accordingly, taking into account all the relevant factors of this case, and given the special financial circumstances that the Respondent is in, the Commissioner has decided to adjust the amount of financial penalty to an amount which would adequately reflect the seriousness of the breach of the PDPA, but at the same time not impose a crushing burden on the Respondent or her family.

37 Although the Commissioner has imposed a lower financial penalty in this case, this is exceptional and should not be taken as setting any precedent for the extension of the same leniency or indulgences in other cases. The Commissioner wishes to remind organisations of their obligations under the PDPA and that it takes a serious view towards any unauthorised sale of personal data.

38 The Commissioner hereby directs the Respondent to pay a financial penalty of S$6,000 within 30 days from the date of the Commissioner's direction.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

Grounds of Decision

## Re Jiwon Hair Salon Pte Ltd and others

## [2018] PDP Digest 331

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1612-B0431
**Decision Citation**: [2018] PDP Digest 331; [2018] SGPDPC 2

***Openness Obligation*** *– Lack of data protection policies and practices*

22 January 2018

### BACKGROUND

1 This case highlights that while the Personal Data Protection Act 2012[1] ("PDPA") seeks to balance the protection of individuals' personal data with the need for organisations to use and share that personal data, compliance with the PDPA also serves to ensure that an organisation keeps data which are of significant commercial importance to it protected and out of the reach of its competitors.

### MATERIAL FACTS

2 This case was triggered by, unusually, a complaint from one of the organisations, Jiwon Hair Salon Pte Ltd ("Jiwon"). Jiwon alleged that a former employee ("Employee K") had misappropriated the names and contact numbers (collectively referred to as the "Personal Data") of its customers by surreptitiously accessing its customer management system ("CMS").

3 An investigation was conducted into Jiwon's complaint and into the following organisations ("Organisations") which Employee K had worked at after leaving Jiwon to determine if indeed Employee K was using the Personal Data from Jiwon's CMS:

1 Act 26 of 2012.

| S/N | Organisation | Start of employment | End of employment |
|---|---|---|---|
| 1. | Jiwon | 9 April 2014 | 15 August 2016 |
| 2 | Next@Ion Pte Ltd | 10 August 2016 | 30 November 2016 |
| 3. | Next Hairdressing Pte Ltd | 1 December 2016 | 16 December 2016 |
| 4. | Initia Pte Ltd | 13 January 2017 | – |

4 In the meantime, Jiwon had instituted an action against Employee K in the State Courts arising out of the facts set out in the complaint and, according to Jiwon, an out-of-court settlement had been entered into. During the investigations, it became clear that none of the Organisations had any policies or practices in place for the protection of the personal data they collected. This decision is solely concerned with the compliance of the Organisations' obligations under s 12(*a*) of the PDPA and the foregoing information on Jiwon's initial complaint serves merely as background information to give context.

## FINDINGS AND BASIS FOR DETERMINATION

### *Whether the Organisation had complied with its obligations under section 12 of the Personal Data Protection Act*

5 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 ("Openness Obligation").

6 During the investigations, it became apparent that the Organisations did not implement any data protection policies or practices. This was admitted to by the Organisations.

7 In the circumstances, I find that, by their own admission, each of the Organisations failed to meet its obligations under s 12(*a*) of the PDPA.

8 I would like to take this opportunity to repeat the exhortations made in *Re M Stars Movers & Logistics Specialist Pte Ltd*[2] ("*M Stars Movers*") to organisations to put in place policies and practices to protect personal data.

2 [2018] PDP Digest 259.

9 The M Stars Movers grounds of decision (at [27] and [28]) explains the need for organisations to put in place data protection policies and practices as follows:

> 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.
>
> An overarching data protection policy will ensure a consistent minimum data protection standard across an organisation's business practices, procedures and activities (*eg*, communications through social media).

## DIRECTIONS

10 Having found that the Organisations are in breach of s 12(*a*) of the PDPA, I am empowered under s 29 of the PDPA to give the Organisations such directions as I deem fit to ensure compliance with the PDPA.

11 In assessing the breach and determining the directions to be imposed on the Organisations, I took into account that the personal data collected by the Organisations were limited to the names and contact numbers of its customers.

12 I have decided to issue the following directions to each of the Organisations:

> (a) to put in place a data protection policy to comply with the provisions of the PDPA within 60 days from the date of this direction; and
>
> (b) to inform the office of the Commissioner of the completion of the above directions within one week of implementation.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

## Grounds of Decision

## Re My Digital Lock Pte Ltd

## [2018] PDP Digest 334

**Coram**: Yeong Zee Kin, Deputy Commissioner
**Case Number**: DP-1612-B0423
**Decision Citation**: [2018] PDP Digest 334; [2018] SGPDPC 3

***Intersection between the law protecting privacy and personal data protection*** *– Right to prevent false publicity (defamation and malicious falsehood)*
***Intersection between the law protecting privacy and personal data protection*** *– Right to prevent publication of private communication*
***Intersection between the law protecting privacy and personal data protection*** *– Right to prevent the appropriation of identity (personality and publicity rights)*
***Intersection between the law protecting privacy and personal data protection*** *– Right to seclusion*
***Powers of investigation*** *– Commissioner's exercise of discretionary investigatory powers – Discontinuation of investigation under section 50(3)*(e) *of the PDPA – Action founded in other areas of privacy*

12 February 2018

1 This is the third complaint lodged by the complainant ("Complainant") against My Digital Lock Pte Ltd ("Organisation"). The first complaint was the subject of the decision in *Re My Digital Lock Pte Ltd*.[1] Investigations were discontinued in respect of the second complaint, as the facts and allegations relied upon in the complaint were closely linked to legal proceedings which were ongoing at the time between the Complainant and the Organisation, and it was determined that the matter was best dealt with through the ongoing legal proceedings. In this third complaint, after a review of the material facts, I exercised my discretion

1 [2017] PDP Digest 146.

under s 50 of the Personal Data Protection Act 2012[2] ("PDPA") to discontinue investigations. I set out hereunder the reasons for the exercise of my discretion in this case.

## BACKGROUND

2 Sometime in October 2015, the Complainant purchased a digital lock from the Organisation for his home. Shortly after, the Complainant and the sole director of the Organisation ("Sole Director") became involved in a dispute concerning alleged defects in the Organisation's product. The Organisation then took out civil action in defamation in relation to certain remarks that were allegedly made by the Complainant concerning the Organisation's business.

3 Subsequently, the Sole Director posted screenshots of WhatsApp messages, as well as photographs, on his personal Facebook page ("Facebook Page"). These WhatsApp messages and photographs were related to the then ongoing dispute between the Organisation and the Complainant. The personal data in the WhatsApp messages comprised the Complainant's contact details, namely, his mobile phone number and residential address.

4 On 4 January 2016, the Complainant lodged a complaint with the Personal Data Protection Commission ("Commission") after discovering the unauthorised disclosure of his personal data on the Facebook Page. In respect of this complaint, a Warning was issued to the Organisation for breaching its obligations under ss 13 and 24 on 4 November 2016. See *Re My Digital Lock Pte Ltd*[3] for the detailed grounds of this decision.

5 On 9 September 2016, before the decision for the first complaint was issued, the Complainant lodged a second complaint concerning the Organisation's disclosure of his personal data on a publicly accessible blog. This blog was the personal blog ("Blog") of the Sole Director who had set it up with the intent to respond to the various allegations made by the Complainant about the Organisation's business. The Sole Director posted images and screenshots of the online allegations that had been made by the

2 Act 26 of 2012.

3 [2017] PDP Digest 146.

Complainant on various websites and forums, and appended his personal response to each of these allegations.

6 One of the images the Sole Director posted on his Blog was a letter sent by the Organisation's solicitors to the Complainant in April 2016. The screenshot was of an open window, in which was displayed a letter and the file name of this document was displayed in the title bar of the open window ("Letter"). The Complainant's name formed part of the file name of the Letter. Although the file name displayed in the window title was not redacted, the Sole Director had taken care to redact the name and residential address of the Complainant in the body of the Letter that was displayed in the open window. Investigations into the matter were discontinued as the matters arising from the complaint would have been more appropriately dealt with as part of the then ongoing legal proceedings between the parties. Any claims or allegations made, or any facts relied upon, by either party would have very likely been relevant to the civil proceedings as the Blog was set up by the Sole Director to refute the alleged defamatory remarks made by the Complainant – this goes to the crux of the civil dispute between the parties.

7 I would, at this juncture, highlight the decision in *Re M Stars Movers & Logistics Specialist Pte Ltd*[4] ("*M Stars Movers*") and reiterate that an organisation cannot be prevented from making reasonable and proportionate responses to defend itself from allegations made against it, even if personal data are disclosed in doing so. In *M Stars Movers*, action was taken against the organisation because the personal data that were disclosed were disproportionate in the circumstances and therefore the organisation was found to have acted unreasonably. In the second complaint, the Complainant had chosen to air his grievances with the Organisation on multiple public websites and forums. As investigations were discontinued, the Commissioner did not have to address the issue whether naming the Complainant in his Blog in an attempt to refute the allegations made would have been a reasonable and proportionate response in the circumstances.

8 The Complainant made his third complaint ("Complaint") on 5 November 2016. This time, the Complainant referred the Commission to a Facebook post where the Organisation had posted a copy of a police

4 [2018] PDP Digest 259.

report that the Organisation's staff had made about a person who was allegedly harassing the staff of the Organisation. The Complainant was named by the Organisation's member of staff as the one who was carrying out such harassing acts.

9 Investigations commenced on 8 December 2016. I subsequently directed that investigations into the case be discontinued and an advisory notice issued to the Organisation. Although my decision was a discontinuance under s 50(3) of the PDPA, I thought it helpful to provide detailed reasons for doing so. This decision touches on issues that are fundamental to the administration and enforcement of the PDPA, namely:

> (a) when does a document containing personal data that is the subject matter of a complaint become one that the Commissioner (or his delegates) will consider exercising enforcement jurisdiction over;
> (b) how does the PDPA sit within the framework of statutory and common law rights that collectively provide safeguards to the privacy of individuals in Singapore; and
> (c) how does the Commissioner discern between a breach of the PDPA that ought to be investigated and cases for which private action in the civil courts enforcing the abovementioned framework of laws provide better remedies to safeguard the privacy of individuals?

## DOCUMENTS CONTAINING PERSONAL DATA

10 We start with the definition of "personal data" in s 2 of the PDPA. This is a broad definition:

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

11 There are certain types of information that in and of themselves are capable of identifying an individual. The *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[5] ("Key Concepts Guidelines") at para 5.10 provides a list of information that is considered to be capable of

5 Revised on 27 July 2017.

doing so. While such information is capable of identifying an individual, it does not necessarily mean that anyone in possession of the information will be able to do so. The touchstone used to compile the list is the one-to-one relationship of the information and the individual. Information on the list is not typically associated with more than one individual, either scientifically (*eg*, biometric signature and DNA profile), by convention (*eg*, NRIC number) or as a matter of social norms (*eg*, personal mobile phone number).

12 At a higher level of abstraction, we consider the question when does a document contain information about an individual? What are the factors that the Commissioner considers in deciding whether the use or disclosure of personal data in documents draws its scrutiny through the lens of the PDPA? The remarks that follow apply not only to textual documents but images (*eg*, photographs that capture the image of an identifiable individual in the *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*[6] at para 4.2) and audiovisual documents (*eg*, CCTV footage in *Re Management Corporation Strata Title Plan No 2956*).[7]

13 In the UK case of *Durant v Financial Services Authority*[8] ("*Durant*"), the Court of Appeal adopted the "biographically significant information" test where the recording of the information goes beyond the mere "putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised". The focus of the information should be the data subject rather than some other person, or some transaction or event in which the data subject may have figured or have had an interest.[9]

14 In a subsequent case of *Edem v The Information Commissioner*,[10] the English Court of Appeal cast doubt on the biographically significant information test as the sole criterion. Without expressly overruling the earlier decision in *Durant*, the court held that the disclosure of the names of three individuals could be withheld on the basis that they constituted

6 Revised on 28 March 2017.

7 [2017] PDP Digest 238.

8 [2003] EWCA Civ 1746.

9 *Durant v Financial Services Authority* [2003] EWCA Civ 1746 at [28].

10 [2014] EWCA Civ 92.

personal data upon which the UK Data Protection Act 1998[11] was applicable. The court, agreeing with the Information Commissioner's Office ("ICO") *Data Protection Technical Guidance*, took the view that it was not "always necessary to consider 'biographical significance' to determine whether data is personal data" – the only time to consider the "biographical significance" of the data is where the information is not "obviously about" an individual or clearly "linked to" him.[12]

15 In assessing whether an unauthorised disclosure or access of information about an individual in a document ought to be one that requires scrutiny under the PDPA, the approach that ought to be taken is to first consider whether the document is clearly about an individual or individuals. Hence, flight manifests that serve the function of conveying information about the individuals on the flight will qualify: see *Re Tiger Airways Singapore Pte Ltd*.[13] Similarly, a letter that is intended to identify a former employee to the organisation's customers will also qualify: see *Re Jump Rope (Singapore)*.[14] As the collection of documents increases, the purpose of recording or conveying information about individuals becomes indisputable. Hence, mishandling of customers' insurance records (*eg*, *Re Ang Rui Song*),[15] and breaches of information systems containing customer or membership records (*eg*, *Re Orchard Turn Developments Pte Ltd*)[16] are cases where the documents were clearly about individuals.

16 Even if a document is not clearly about the individual, such as the documents in *Durant* which pertained to Mr Durant's complaint to the Financial Services Authority ("FSA") about the conduct of Barclays Bank or about the FSA's own conduct in their investigations of his complaint, the Commissioner would consider whether the information is biographically significant. Consider instant messaging communications, which will contain the identifier associated with the author of each message: see *Re Executive Coach International Pte Ltd*.[17] These identifiers are automatically inserted into the communication as a function of the communication system.

11 c 29.
12 *Edem v The Information Commissioner* [2014] EWCA Civ 92 at [21].
13 [2018] PDP Digest 166.
14 [2017] PDP Digest 154.
15 [2018] PDP Digest 236.
16 [2018] PDP Digest 223.
17 [2017] PDP Digest 188.

Similarly, an exchange of social media posts will contain identifiers of who wrote each post, as will e-mails contain the sender and intended recipients' names and e-mail addresses. In and of themselves, such identifiers are intended to identify the originator (or recipient) but does it mean that the *purpose of each such message* is to convey information about the originator by reason only of the inclusion of the identifier? I do not think so. It is necessary to consider the content of the message. The content of the message must convey information about one or more individuals. Thus in *Re Black Peony*,[18] it was decided that private communications such as WhatsApp messages *per se* will not invariably be considered personal data.

17 This approach applies to all types of documents, textual as well as multimedia. This may be relevant in cases in which the Commissioner exercises his discretion to suspend, discontinue or refuse to conduct an investigation.

18 At this juncture, I take the opportunity to highlight that an individual has two avenues through which he may address his concerns of a potential breach of the PDPA by an organisation. The individual may submit a complaint to the Commission. Where the individual has suffered loss or damage directly as a result of the contravention, the individual may commence civil proceedings against the organisation under s 32 of the PDPA.

19 Where the individual chooses to lodge a complaint with the Commission, the Commissioner (and his delegates) has discretion under s 50(3) of the PDPA to suspend, discontinue or refuse to conduct an investigation. One of the circumstances in which the Commissioner may exercise his discretion under s 50(3) of the PDPA is where the Commissioner deems that the severity of the potential breach does not warrant taking any further action. Data protection regulators in other jurisdictions, such as the UK ICO,[19] similarly take the same approach, as clearly every single data protection complaint cannot be investigated. In determining the severity of the potential breach, the Commissioner may consider, amongst other things, the nature of the personal data affected, the number of people affected, whether the breach is due to systemic issues and

18 [2017] PDP Digest 218.

19 UK Information Commissioner's Office, *How we deal with complaints and concerns – A guide for data controllers* at p 4.

the likely effect on the individuals concerned. The biographical significance test would be relevant when considering the nature of the personal data affected and the likely effect on the data subject.

20 In the present case, the document concerned was a police report made by a member of the Organisation's staff concerning harassing conduct purportedly carried out by the Complainant. The disclosure of the Complainant's identity was therefore one of the purposes of the report and since the allegation in the report was about the Complainant's purportedly harassing conduct, the content of the report was therefore potentially of biographical significance. I have nevertheless decided to exercise my discretion in this case to discontinue investigations in this matter. The following discussion will explain my exercise of discretion. A caveat ought to be inserted at this juncture that this is not intended to be a comprehensive compendium of all considerations in the exercise of discretion. There will be future cases where different aspects of the discretion will be explained, within the factual matrix of those cases.

## INTERSECTION BETWEEN THE LAW PROTECTING PRIVACY AND PERSONAL DATA PROTECTION

21 In order to explain the exercise of my discretion to discontinue investigations, it is necessary to understand the interaction between the applicable common law principles – by which I mean also to include statutory torts – that protect privacy and the operations of the PDPA. Even if the information in a document has a purpose of conveying information about an individual, it is not necessarily the case that the most appropriate remedies are in the civil administrative enforcement provisions of the PDPA. While it has oft been said that there is no right to privacy under common law, this statement ought to be re-examined in the light of developments in both the common law and statutory torts in the recent past. Without going into a lengthy dissertation, I posit that while it is probably still true that the common law does not recognise a *general right* to privacy, there exists today a framework of common law and statutory torts that collectively protect an individual's privacy. Individuals are therefore able to prosecute their claims for invasions into their privacy by private action before the civil courts much more effectively today than in the past.

22 The Singapore courts have not made any explicit pronouncements that a *general tort of privacy* exists nor that there is explicit provision for the

protection of privacy as a fundamental right in our Constitution;[20] neither is there an omnibus privacy legislation in our statute books.[21] The starting point in Singapore is therefore not very different from the common law. *Kaye v Robertson*[22] ("*Kaye v Robertson*") has often been cited as authority for the proposition that there is no right to privacy in the common law. *Kaye v Robertson* was a case which involved journalists intruding into the hospital room of a well-known actor and taking photographs of him. The UK Court of Appeal acknowledged that "[it] is well-known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person's privacy".[23] This position was confirmed in *Wainwright v Home Office*[24] when the House of Lords declined to recognise a general right of privacy which would extend to physical privacy interferences. Although our Court of Appeal traversed the authorities in the case of *ANB v ANC*[25] ("*ANB v ANC*"), the question whether a common law right of privacy should be recognised was intentionally left open.[26]

23 Privacy, as a standalone common law right, is steadily gaining recognition in some parts of the Commonwealth. Recent developments in Canada and New Zealand that recognise a general common law right to seclusion are discussed in a subsequent section: see discussion below at [28]–[29]. Most recently, the Indian Supreme Court in the case of *Justice KS Puttaswamy (Retd) and ANR v Union of India*[27] ("*Puttaswamy*") recognised the right to privacy as a constitutional right. Although the decision did not address the question whether privacy rights were enforceable as a common law tort, it was clear that the majority of the Supreme Court felt that the right to privacy was a fundamental right protected by the Indian Constitution.

---

20 Constitution of the Republic of Singapore (1999 Rev Ed).

21 See Gary Chan Kok Yew & Lee Pey Woan, *The Law of Torts Singapore* (Academy Publishing, 2nd Ed, 2015) at para 16.011.

22 [1991] FSR 62.

23 *Kaye v Robertson* [1991] FSR 62 at 66, *per* Glidewell LJ.

24 [2004] 2 AC 406.

25 [2015] 5 SLR 522.

26 See *ANB v ANC* [2015] 5 SLR 522 at [20]–[23].

27 Writ Petition (Civil) No 494 of 2012.

24 It is unlikely that our courts would take the same approach as in *Puttaswamy*. In *Lim Meng Suang v Attorney-General*,[28] the Singapore Court of Appeal held that the right to privacy and personal autonomy should not be read into the phrase "life or personal liberty" in Art 9 of the Singapore Constitution.[29] The Court of Appeal made it clear that there is unlikely to be a constitutional right to privacy; the appellants cannot "obtain by the (constitutional) backdoor what they cannot obtain by the (private law) front door".[30] However, the Court of Appeal left it open for there to be a right to privacy "developed by way of the private law on privacy instead".[31]

25 While our courts have not recognised the existence of a general right to privacy that is an actionable tort, or a fundamental right protected by our Constitution, that is not to say that our laws do not protect different aspects of privacy. An appreciation of how privacy is protected by a framework of common law and statutory torts is a necessary primer for understanding the interaction between the common law principles that protect privacy and the operation of the PDPA. It is apposite to preface the discussion by drawing a distinction between those torts that indirectly protect privacy interests (*eg*, trespass to the person or land and nuisance), and the bundle of rights that a general right to privacy protects. It is the latter that we train our focus on.

26 What is privacy? A useful definition with which to commence our discussion is that which was provided by Samuel D Warren and Louis D Brandeis – the right to be let alone.[32] A helpful framework for discerning the contours of this right was offered by William L Prosser ("Prosser"):[33]

> (a) the right to seclusion – the right to prevent intrusions into one's seclusion that exists independently of the tort of trespass to person or property;
>
> (b) the right to prevent publication of private communication – recent common law developments have started to recognise the existence of this right independently of the law of confidentiality;

---

28 [2015] 1 SLR 26.

29 *Lim Meng Suang v Attorney-General* [2015] 1 SLR 26 at [44]–[47].

30 *Lim Meng Suang v Attorney-General* [2015] 1 SLR 26 at [49]

31 *Lim Meng Suang v Attorney-General* [2015] 1 SLR 26 at [49].

32 See Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4(5) Harvard L Rev 193 at 195.

33 See William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 389.

(c) the right to prevent the appropriation of identity; and
(d) the right to prevent false publicity.

27 The Prosser categorisation provides a useful framework for examining the different aspects of privacy. It is necessary to understand how this bundle of rights are currently protected by common law and statutory torts in order to appreciate the dynamics between remedies under these laws protecting an individual's privacy and the Commissioner's role in the enforcement of the PDPA, which protects informational privacy and therefore sits within the penumbra of the laws protecting privacy.

### *Right to seclusion*

28 Intrusion upon seclusion or solitude involves an invasion of a victim's private space or affairs. Some torts that are premised on trespass to property or person protect aspects of the right to seclusion, but to be effective, this right ought not to be dependent on an invasion of one's person or property. The tort of privacy based on the right to seclusion has been recognised in other countries. In New Zealand, the High Court recognised the common law tort of intrusion upon seclusion as a standalone tort in *C v Holland*[34] ("*C v Holland*"). In that case, the claimant was a young woman who suffered deep distress when she discovered that her boyfriend's flatmate had covertly installed a camera in the roof cavity above the bathroom to film her undressing and showering. To establish a claim under the tort of intrusion upon seclusion, a claimant had to show:[35]

(a) an intentional and unauthorised intrusion;
(b) into seclusion (namely, intimate personal activity, space or affairs);
(c) involving infringement of a reasonable expectation of privacy; and
(d) that is highly offensive to a reasonable person.

29 In Canada, the courts have also recognised a common law right of action for intrusion upon seclusion in the case of *Jones v Tsige*[36] ("*Jones v Tsige*"). In that case, the defendant, who was in a relationship with the

34 [2013] 3 LRC 78.
35 See *C v Holland* [2013] 3 LRC 78 at [94].
36 (2012) ONCA 32.

claimant's former husband, and who worked for the same bank as the claimant but in a different branch, used her workplace computer to gain access to the claimant's private banking records 174 times, for the alleged purpose of confirming whether the claimant's former husband was paying child support. In confirming the existence of the intrusion-based privacy tort, the Ontario Court of Appeal adopted as essential elements the formulation in §652 of the US Restatement of the Law, Second, Torts (1977):[37]

> One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person.

30 In Singapore, the High Court, in the case of *Malcomson Nicholas Hugh Bertram v Mehta Naresh Kumar*,[38] was perhaps a little ahead of the times when it took a decidedly different turn from the general common law position by recognising a tort of intentional harassment. The elements of this tort were (a) knowingly engaging in (b) a sufficiently repetitive course of conduct that would (c) cause worry, emotional distress or annoyance to another person.[39] The Court of Appeal in *Tee Yok Kiat v Pang Min Seng*[40] did not question the existence of the tort of intentional harassment. The similarities and differences between this tort of intentional harassment and the more recent torts of intrusion upon seclusion would have provided ample fodder for commentary. Unfortunately, while the New Zealand and Canadian courts were establishing equivalent torts of privacy, the High Court in the subsequent case of *AXA Insurance Singapore Pte Ltd v Chandran s/o Natesan*,[41] cast doubt on the existence of this common law right and called for legislative intervention if such a right ought to be recognised.

31 The tort of harassment is now enshrined in ss 3 and 4 of the Protection from Harassment Act[42] ("POHA"). The POHA had expressly

37 *Jones v Tsige* (2012) ONCA 32 at [70].

38 [2001] 3 SLR(R) 379.

39 *Malcomson Nicholas Hugh Bertram v Mehta Naresh Kumar* [2001] 3 SLR(R) 379 at [31].

40 [2013] SGCA 9.

41 [2013] 4 SLR 545 at [8]–[10].

42 Cap 256A, 2015 Rev Ed.

abolished the common law tort of intentional harassment and established that no civil proceedings shall be brought for the tort of harassment except as a statutory tort under s 14 of the POHA. The POHA also introduced a statutory tort of unlawful stalking: s 7. The operation of these sections is briefly described in *Ting Choon Meng v Attorney-General*:[43]

> (a) s 3 makes it an offence for a person to behave or communicate in a 'threatening, abusive or insulting' way with the intention of causing, and actually causing, 'harassment, alarm or distress' to a victim;
> (b) s 4 makes it an offence to behave or communicate in a 'threatening, abusive or insulting' way towards a victim who is likely to be caused 'harassment, alarm or distress'; and
> (c) s 7 makes 'unlawful stalking' an offence, and defines this as engaging in a course of conduct which involves acts or omissions associated with stalking and which causes 'harassment, alarm or distress' to a victim, provided that there was an intention to cause such 'harassment, alarm or distress' or at least knowledge that this was a likely outcome.

32 Collectively, these statutory provisions can now be relied upon to protect one's seclusion from intrusion. These are still relatively new statutory torts and time will tell if they provide the same umbrella of protection as a general tort of intrusion upon seclusion. If the excesses of the paparazzi caused alarm or distress to Mr Kaye in *Kaye v Robertson*, he may now resort to the statutory tort of harassment for relief. Similarly, the victim in *C v Holland* may now seek relief against her boyfriend's flatmate under the tort of unlawful stalking. The protection offered by these statutory torts no doubt covers physical intrusions, but may extend to online activities where the *communication content* amounts to harassment or stalking conduct. In *Benber Dayao Yu v Jacter Singh*[44] ("*Benber Dayao Yu*"), it was held that "harassing conduct on the Internet, such as those in the Web post in the present case, would be covered by ss 3 and 4 of the POHA".

33 However, the victim in *Jones v Tsige* probably may not be able to resort to these statutory torts to safeguard her bank accounts from the prying eyes of the defendant. But there is room for the PDPA, which deals with *informational privacy*, to operate in conjunction with the aforementioned statutory torts to protect intrusions into seclusion. The

43 [2016] 1 SLR 1248 at [15].
44 [2017] 5 SLR 316 at [25].

factual matrix of *Jones v Tsige* can potentially be a breach of the protection obligation on the part of the bank (but may provide no reliefs against the former husband or his lover, the defendant, as they were acting in a domestic or personal capacity). Likewise, the factual matrix of *Kaye v Robertson* can give rise to a claim for collection of personal data without consent. Both of these breaches can now be enforced as private actions under s 32 of the PDPA. The right of private action under the PDPA protects *informational* privacy which is complementary to but distinct from the protection of one's seclusion, although these rights may overlap and co-exist.

34 It is open to debate whether there is still room for a common law tort of intrusion upon seclusion, although the contours of such a tort will be heavily influenced by the statutory torts under the POHA and PDPA. This is not the place nor is it my intention to discuss the similarities and differences between the range of conduct prohibited by the statutory torts under the POHA and PDPA, and those categories prohibited by a common law tort that prevents intrusion upon seclusion. Before leaving this category, it suffices for me to make the following observations. *First*, the state of our laws does not leave one's right to seclusion unprotected; as can be seen from the foregoing discussion, there are statutory torts that collectively offer a significant degree of protection of one's seclusion from unwanted intrusion. These are early days and the jurisprudence can be expected to grow as more cases are brought before the courts, and more commentaries are published. *Second*, a plaintiff seeking relief against his intruder by filing a civil claim can pursue one or more of the statutory torts in the POHA and PDPA, whereas a complaint lodged with the Commission is limited to redress for PDPA breaches. *Third*, our courts may well take a leaf from the common law developments in Canada and New Zealand and find sufficient room for the development of a *general* tort of intrusion into seclusion that complements the statutory torts under the POHA and PDPA. This development of the common law may only be declared by the courts, and then only when the appropriate case goes before them. Therefore, if the true mischief is an intrusion upon one's seclusion, a civil claim before the courts is more likely to yield an effective set of reliefs than a complaint to the Commission.

***Right to prevent publication of private communication***

35 Another strand of development in the right of privacy is the recognition of the right to prevent publication of private communication. This has now been recognised as a new cause of action distinct from an action for breach of confidence in two House of Lords cases: see *Campbell v MGN Ltd*[45] ("*Campbell*") and *Douglas v Hello! Ltd*[46] ("*Douglas*"). In *Campbell*, the House of Lords held that where the invasion of privacy is occasioned by a wrongful disclosure of personal information, "the essence of the tort is better encapsulated now as misuse of private information".[47] In *Douglas*, it was explicitly recognised that "traditional" breach of confidence and misuse of private information had become separate and distinct wrongs.[48] The key development in this tort is, to my mind, the availability of remedies even where the private communication does not have the necessary quality of confidence, which had hitherto been the death knell to any action based on a breach of confidentiality.[49] While confidentiality protects secrecy, the cause of action for misuse involves the identification of private information as "something worth protecting as an aspect of human autonomy and dignity".[50]

36 While this development in the UK may be viewed as being necessitated by their obligation to give effect to the European Union

---

45 [2004] 2 AC 457.

46 [2008] 1 AC 1.

47 *Campbell v MGN Ltd* [2004] 2 AC 457 at [14], *per* Lord Nicholls of Birkenhead.

48 *Douglas v Hello! Ltd* [2008] 1 AC 1 at [255], *per* Lord Nicholls of Birkenhead.

49 See *Coco v AN Clark (Engineers) Ltd* [1968] FSR 415.

50 *Campbell v MGN Ltd* [2004] 2 AC 457 at [50]. As Lord Hoffman said at [51]:

> [T]he new approach takes a different view of the underlying value which the law protects. Instead of the cause of action being based on the duty of good faith applicable to confidential personal information and trade secrets alike, it focuses upon the protection of human autonomy and dignity – the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people.

See also *Tugendhat and Christie, The Law of Privacy and the Media* (Mark Warby QC, Nicole Moreham & Iain Christie eds) (Oxford: Oxford University Press, 2nd Ed, 2011) at para 5.04.

Human Rights Convention as enacted in the UK Human Rights Act 1998,[51] the Singapore Court of Appeal in *ANB v ANC* observed that the English common law had recognised a right to privacy as long ago as the 1990 decision of *Attorney-General v Observer Ltd*.[52] The relationship between the right of privacy and breach of confidence was also articulated in *Hellewell v Chief Constable of Derbyshire*:[53]

> If someone with a telephoto lens were to take from a distance and with no authority a picture of another engaged in some private act, his subsequent disclosure of the photograph would, in my judgment, as surely amount to a breach of confidence as if he had found or stolen a letter or diary in which the act was recounted and proceeded to publish it. In such a case, the law would protect what might reasonably be called a right of privacy, although the name accorded to the cause of action would be breach of confidence.

37 The Court of Appeal in *ANB v ANC* recognised that such a right had emerged in the UK from the law of breach of confidence. Developments in other common law jurisdictions – New Zealand was specifically mentioned – and the statutory developments in Singapore – principally, the enactment of the POHA and PDPA – were referred to as signalling an increasing recognition of the need to protect personal privacy.[54] Whilst the Court of Appeal stopped short of making an express determination on the issue as it was deciding an interlocutory appeal, it recognised that the question of "whether we should afford, like the courts in England and various other jurisdictions, protection to one's privacy by way of the law of confidence regardless of whether such a right is guaranteed under the Constitution … [the] extent to which we should adopt such jurisprudence, *ie*, the circumstances under which the law of confidence would extend its protection to private information acquired without consent" gave rise to serious questions to be tried. The Court of Appeal concluded by cautioning that it was "by no means endorsing or encouraging, the identification of a right to protection of private information under our law of confidence".[55]

38 This right to prevent misuse of private communication and informational privacy often – but not necessarily always – coexist. Private

---

51 c 42.

52 [1990] 1 AC 109.

53 [1995] 1 WLR 804 at 807; [1995] 4 All ER 473 at 476.

54 See *ANB v ANC* [2015] 5 SLR 522 at [22].

55 *ANB v ANC* [2015] 5 SLR 522 at [23].

communications that interlocutors are keen to prevent misuse of often contain information that is personal or intimate, and frequently personal information of a biographical nature. A couple of observations may be made. *First*, the right to prevent the misuse of *private information* seeks to prohibit the publication of information that was meant to be private. The PDPA prevents, in this context, disclosure of *personal data* without authority. The range of communications that the common law right protects is broader, as it extends beyond personal information to communications content. For example, an intimate conversation within the confines of a taxicab may not contain any personal information. The right to prevent its publication lies with the common law right to prevent publication of private information, not with the PDPA. Also, a document that contains personal information incidentally (*eg*, names and contact details in a letter or e-mail) may not be one that the Commissioner will consider exercising enforcement jurisdiction over: see discussion above, at [14] *et seq*, on whether the document conveys personal information or the information is biographically significant.

39 *Second*, the common law right will protect private information *in the nature of personal data* from publication even if the information is publicly available. Thus, the taking of a photograph in a public space may be an infringement of privacy, if it intrudes into the individual's personal space:[56] "the widespread publication of a photograph of someone which reveals him to be in a situation of humiliation or severe embarrassment, even if taken in a public place, may be an infringement of the privacy of his personal information". The taking of a photograph in a public place would attract the "publicly available exception"[57] in the PDPA, which obviates the need to obtain consent and provide notification.[58] Although consent and notification are not required, s 18(*a*) of the PDPA may still operate to limit the collection, use or disclosure of such personal data to appropriate purposes. In determining the appropriateness of any particular purpose, considerations of the data subject's objective expectation of privacy may

56 *Campbell v MGN Ltd* [2004] 2 AC 457 at [75], *per* Lord Hoffman.

57 As found in para 1(*c*) of the Second Schedule, para 1(*c*) of the Third Schedule, and para 1(*d*) of the Fourth Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012).

58 See examples in the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at para 12.63.

conceivably be entertained. In this manner, the PDPA may provide similar protection to publicly available personal data as the common law. Personal data that were publicly available at the time they were collected can continue to be used or disclosed without the need for consent, even if the personal data are subsequently taken offline.[59]

40 It may therefore be said that an interlocutor who wishes to prevent misuse of his private communication should look towards the new tort established in *Campbell* and *Douglas*, with an eye on the PDPA where the private information is in the nature of personal data. The same observations made in respect of the right to prevent intrusion upon seclusion may be reiterated here: a private claimant prosecuting his case in the civil courts can plead both the common law tort to prevent publication of private information as well as pursue a private claim based on breaches of the PDPA. This not only provides him with a potentially more comprehensive set of reliefs, but will also provide the courts with the opportunity to consider adopting into our case law the same common law right in *Campbell* and *Douglas*. The Commissioner does not have the *vires* to extend its jurisdiction in these directions when investigating into a complaint.

### *Personality rights*

41 I deal with the final two of Prosser's categories collectively, as both relate to the protection of one's personality from misuse or abuse.

#### *Right to prevent appropriation of identity (personality and publicity rights)*

42 The right of publicity is the right of an individual to control the commercial exploitation of an individual's fame or identity.[60] This extends to his name, image, voice, signature, or any other distinguishing characteristic which identifies him, and as such are considered personal data. Unsurprisingly, the Key Concepts Guidelines at para 5.10 similarly lists data that on their own can identify an individual as "unique identifiers": *eg*, full name, facial image and voice of an individual. Needless

59 See the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised on 27 July 2017) at para 12.61.

60 See David Tan, "Image Rights and Data Protection" (NUS Law Working Paper Series 2017/010) at p 4.

to say, there must be commercial value in these characteristics in order for the right to publicity to provide a remedy for financial loss suffered as a result of unauthorised use.[61]

43 The right of publicity may be protected under intellectual property law, specifically, the law of passing off. Individuals may bring a cause of action under the tort of passing off to prevent false and unauthorised celebrity endorsements of goods and services. In the case of *Irvine v Talksport Ltd*,[62] the English High Court acknowledged the expansion of the law of passing off to include cases of false endorsement. In so far as an individual acquires a valuable reputation or goodwill, the law of passing off will protect it from unlicensed use by other parties. However, the claimant must be able to prove two interrelated facts: (a) at the material time, the claimant had significant reputation or goodwill, and (b) the actions of the defendant gave rise to a false message which would be understood by a not insignificant section of his market that his goods have been endorsed, recommended or approved of by the claimant.[63]

44 Given that there is a right of private action under the PDPA, it has been commented that the PDPA confers an "incidental personality right" on the individual, similar to the right of publicity.[64] Whether the PDPA effectively creates a right of publicity regime in Singapore is open to debate. This and other pertinent issues are detailed in two articles and I can do no better than to refer the interested student to these commentaries: (a) David Tan, "Image Rights and Data Protection";[65] and (b) Gilbert Leong, Foo Maw Juin & Kenneth Fok, "Protecting the Right of Publicity under the PDPA".[66]

---

61 See the exposition of the law in the US in relation to publicity rights in *Tugendhat and Christie, The Law of Privacy and the Media* (Mark Warby QC, Nicole Moreham & Iain Christie eds) (Oxford: Oxford University Press, 2nd Ed, 2011) at paras 3.110–3.114.

62 [2002] 1 WLR 2355.

63 *Irvine v Talksport Ltd* [2002] 1 WLR 2355 at [46].

64 David Tan, "Image Rights and Data Protection" (NUS Law Working Paper Series 2017/010) at p 1.

65 NUS Law Working Paper Series 2017/010.

66 [2017] PDP Digest 293.

*Right to prevent false publicity (defamation and malicious falsehood)*

45 The tort of false light publicity has been described as protecting interests similar to reputation, whilst having the same overtones of mental distress as in defamation.[67] At the heart of this false light tort is the need to protect the reputation of the person. Reputation is protected by English law in a number of ways, including malicious falsehood, passing off and defamation. In *Tolley v JS Fry & Sons Ltd*,[68] an amateur golfer, who was depicted without his knowledge or consent in a newspaper advertisement for a Fry's chocolate bar, sued in defamation arguing that the advertisement implied that he had compromised his reputation and status as an amateur golfer. Ultimately the House of Lords held in favour of the amateur golfer for defamation.

46 In Singapore, there has not been any express recognition of a tort of false light publicity, nor any indication that the PDPA was formulated to encompass such a tort. If the case of *Chiam See Tong v Xin Zhang Jiang Restaurant Pte Ltd*[69] ("*Chiam See Tong*") is taken to set any precedent, it would be that any such rights are likely to be found in the areas of the law of defamation. In *Chiam See Tong*, the plaintiff successfully sued in defamation for damages and an injunction when a photograph taken of him at a restaurant for a charity fund-raiser was subsequently used by the defendant as advertisements. It was held that to the ordinary reader, the photograph suggested that the plaintiff had consented to publicise the restaurant.[70]

47 Recently, the English Court of Appeal in *Prince Moulay Hicham Ben Abdullah Al Alaoui of Morocco v Elaph Publishing Ltd*[71] held that a data protection claim could be linked to a defamation claim for the reason that they were different causes of action which were directed to protecting different aspects of the right to private life, and the relevant provisions of the UK Data Protection Act 1998 included the aim of protection from

67 William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 400.

68 [1931] AC 333.

69 [1995] 1 SLR(R) 856.

70 If *Irvine v Talksport Ltd* [2002] 1 WLR 2355 is followed in Singapore, a plaintiff in a similar case in Singapore may be able to sue both under the tort of defamation and passing off.

71 [2017] 4 WLR 28.

being subjected unfairly and unlawfully to distress.[72] It would be too much of an extrapolation to read into this case – which was essentially an interlocutory appeal dealing with the issue of whether amendments to pleadings ought to be permitted – anything beyond the proposition that these are parallel remedies which the plaintiff may legitimately pursue.

48 It is in the area of personality rights that the area of overlap between the PDPA and common law rights is the greatest, since both operate on information that is essentially personal data. This is also the area where the contours between any common law right – this area of law is more developed in the US than in the rest of the common law world – and statutory rights under the PDPA have yet to come under judicial scrutiny in Singapore. Based on the available commentary, the following observations may be made.

49 It has been observed that an individual may not have recourse under the PDPA if the personal data are found in a publicly available space, even where an individual's fame has been commercially exploited.[73] It has also been pointed out that the definition of "personal data" does not adequately deal with the "associative value" that celebrities bring to products and services.[74] Consequently, one may draw the conclusion that private action under the PDPA will probably have limited chance of successfully preventing the classical scenario in which celebrities seek to prevent misuse or abuse of their personality when their identity is taken from a publicly available source.[75]

50 Private individuals are likely to have more success in relying on the PDPA to prevent misuse or abuse of their identity on the basis of use or disclosure without consent. But these are not what the cases on publicity rights thus far deal with. Perhaps the PDPA and the right of publicity are

---

72 *Prince Moulay Hicham Ben Abdullah Al Alaoui of Morocco v Elaph Publishing Ltd* [2017] 4 WLR 28 at [43].

73 See David Tan, "Image Rights and Data Protection" (NUS Law Working Paper Series 2017/010) at p 15 and Gilbert Leong, Foo Maw Juin & Kenneth Fok, "Protecting the Right of Publicity under the PDPA" [2017] PDP Digest 293 at 297.

74 David Tan, "Image Rights and Data Protection" (NUS Law Working Paper Series 2017/010) at p 4.

75 See *Tolley v JS Fry & Sons Ltd* [1931] AC 333 and *Chiam See Tong v Xin Zhang Jiang Restaurant Pte Ltd* [1995] 1 SLR(R) 856.

means to different ends – while the right of publicity seeks to protect the commercial value of the name or image of the individual, the PDPA seeks to hold organisations accountable for the proper and respectful handling of personal data, by imposing a standard of conduct that permits reasonable use, processing or disclosure while preventing misuse or abuse of personal data. This distinction may, in future, guide the Commissioner's exercise of discretion when considering whether to commence investigations into complaints with personality rights undertones.

51 To be clear, while I have mentioned some causes of action above which may not as yet be recognised by the Singapore courts, I would exercise my discretion under s 50(3) to suspend, discontinue or refuse to conduct investigations where I believe there is a more appropriate cause of action which is recognised under Singapore law. But it is necessary to emphasise that our laws provide existing options to protect the privacy of an individual and this is an area that is expected to evolve. The PDPA deals with informational privacy and it would be a mistake to distort it in order to address privacy issues that it was not meant to address. Maintaining a macro perspective is necessary for the law in this area to develop.

## COMMISSIONER'S EXERCISE OF DISCRETIONARY INVESTIGATIVE POWERS IN THIS CASE

52 It is against this backdrop of common law and statutory torts that collectively protect privacy rights that I explain the exercise of my discretion in this case.

### *Commissioner's discretionary investigative powers*

53 Section 50 of the PDPA provides me with the powers of investigation to determine whether an organisation is in breach of the PDPA. The powers of investigation are spelt out in the Ninth Schedule to the PDPA. Section 50(3) provides me a discretionary power to suspend, discontinue or refuse to conduct an investigation under specific circumstances. The relevant circumstance in this case is:

> (*e*) the Commission is of the opinion that —
>
> (i) a complaint is frivolous or vexatious or is not made in good faith; or

(ii) any other circumstances warrant refusing to conduct, suspending or discontinuing the investigation.

54 In this case, the Complainant and the Organisation were engaged in civil proceedings before the District Courts. I understand that those proceedings have now been settled. The prime consideration is whether the subject matter of the present Complaint is better resolved through the judicial process or by an investigation into alleged breaches of the PDPA.

### *Action founded in the other areas of privacy*

55 Having considered the Complaint, I came to the view that the true nature of the Complainant's claim is for protection of his privacy which extends beyond protection of his personal data (which in the Complaint to the Commission involves no more than the disclosure of his name), and thus this is not the appropriate office to investigate his claims. This is where the foregoing (somewhat lengthy) discussions about the interaction of the law on data protection and privacy become relevant.

56 This Complaint is the third complaint made by the Complainant against the Organisation. The alleged infringement concerns the posting of a police report made by a member of the Organisation's staff containing the Complainant's name on Facebook, effectively suggesting that the Complainant was the culprit who carried out the online attacks and harassing acts. The Complainant is essentially alleging in this complaint that his reputation is affected by the Facebook post, because the disclosure of his name in the police report is akin to an accusation by the Organisation that the Complainant had been harassing the victim. All this takes place against the backdrop of a civil dispute between the Complainant and Organisation.

57 The immediate complaint raises issues relating to false light publicity that (as discussed above) lies within the domain of the law of defamation, which seems to be the branch of common law that is most appropriate for the development of rights to prevent false light publicity. The personal data that is disclosed is the Complainant's name. The rest of the police report details conduct that is attributed to him which may be of biographical significance.

58 While it is possible for me to investigate into whether the circumstances leading to the disclosure of the police report involved

unreasonable conduct on the part of the Organisation, it is these same considerations that led me to conclude that addressing this one question would not be the most effective means of settling the dispute between the Complainant and the Organisation. As explained in *M Stars Movers*, an organisation cannot be prevented from defending itself on the same public forum that a complainant chooses to ventilate any dissatisfaction he may have against it. Disclosure of personal data may sometimes be necessary; and it is only when disclosure is a disproportionate response on the part of the organisation that the matter will be investigated under the PDPA. In order to determine whether to commence investigations, it becomes necessary to consider the allegations flowing between the complainant and the organisation, as well as the history of dissatisfaction between them. Given the history between the Complainant and the Organisation, resolving the dispute over the publication of the police report on Facebook is unlikely to settle the underlying dispute between them.

59 In the final analysis, the history of exchanges between the Complainant, the Sole Director and the Organisation discloses issues that can be better addressed before the courts. The legal issues that are potentially raised touch on the Complainant's expectations of privacy which, from our foregoing discussion, is protected by a framework of common law and statutory torts. I am unable to venture beyond the boundaries of the PDPA; the courts face no such constraint. The crux of the Complaint is that of publication of alleged defamatory remarks in a police report. A resolution of the underlying dispute relies on the framework of laws protecting privacy rights rather than the manner in which personal data are managed by the Organisation. Therefore, I did not think that this case was suitable for investigations under the PDPA and exercised my discretion under s 50(3)(*e*)(ii) of the PDPA to discontinue investigations.

60 The true nature of the Complaint revolves around the dispute between the Complainant and the Organisation over the Complainant's alleged online attacks and harassing acts. From the foregoing survey of our privacy laws, this is not an area that is exclusively within the domain of the PDPA. The POHA is potentially relevant at least as an *existing* statutory tort; much more the potential of a common law right to privacy as in *C v Holland* or *Jones v Tsige*.

61 Indeed, it is specifically this category of cases that the PDPA was not meant to cover. In the parliamentary debates leading to the enactment of the PDPA, it was mentioned by Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts (as he then was) that:[76]

> On Mr Zaqy Mohamad's suggestion to cover cyber-bullying and other undesirable online behaviour, the Bill is concerned with regulating the management and the protection of personal data. It does not govern other actions of individuals online. *This would be more appropriately addressed by other laws.* [emphasis added]

62 I can do no better than to echo the Minister's statement. I do not think that the answer lies within the PDPA. On the precedent established in *Benber Dayao Yu*, the answer today lies in ss 3 and 4 of the POHA: see [31] above.

63 Accordingly, for the reasons set forth above, I decided to exercise my discretion under s 50(3) of the PDPA to discontinue investigations into this Complaint and issue an advisory notice to the Organisation.

**YEONG ZEE KIN**
**Deputy Commissioner**
**Personal Data Protection Commission**

76 *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89 (Assoc Prof Dr Yaacob Ibrahim) at p 41.

Case Summary

# RE SOHO TS PTE LTD (HERITAGE@CLARKE QUAY)

***Consent Obligation*** *– Collection and use of personal data without consent – Organisation collected and used credit card details provided through third-party booking website to charge customer*

2 April 2016

## BACKGROUND

1 The Complainant had made a booking for an accommodation with the Organisation via a third-party website, <www.booking.com>, under non-amendable, non-cancellable and non-refundable terms and conditions. As the Complainant was a corporate client, the Organisation had offered him a lower corporate rate if he made the booking directly with the Organisation. The Complainant accepted this offer.

2 However, when the Complainant subsequently cancelled the booking, the Organisation used his credit card details provided through the third-party website to charge the Complainant the booking fee in accordance with its terms and conditions. The Complainant disputed this transaction and managed to receive a chargeback from the credit card company for a full refund from the Organisation.

3 The Complainant then proceeded to lodge a complaint with the Personal Data Protection Commission against the Organisation for collecting and using his credit card details without his authorisation to charge him for the cancelled hotel room booking.

## ISSUE

4 The issue is whether the Organisation was in breach of the Consent Obligation[1] by collecting and using the personal data of the Complainant without consent.

---

1 Pursuant to s 13 of the Personal Data Protection Act 2012 (Act 26 of 2012).

## FINDINGS

5 In consideration of the facts, the Deputy Commissioner takes the view that the Complainant is deemed to have given consent to the Organisation for the collection and use of his credit card details when he made the initial booking. Since the Organisation's collection and use of the Complainant's personal data to process payment for his booking were in accordance with the website's terms and conditions, and were legitimate, the Organisation was not found to be in breach of the Consent Obligation under the PDPA.

Case Summary

# RE SG VEHICLES ASIA PTE LTD

***Consent Obligation*** *– Disclosure of personal data for marketing purposes without consent – Whether publicly available exception applies*
***Consent Obligation*** *– Withdrawal of consent*

13 June 2016

## BACKGROUND

1 The Organisation is a car retailer. The Complainant's father had purchased a vehicle from the Respondent and the Complainant agreed to pose for a photo with the vehicle together with his family in a public car park outside the premises of the Organisation's office.

2 The Complainant subsequently discovered that the Organisation had published the photograph on its website as a testimonial for customer satisfaction with its services. According to the Complainant, he had sent written requests to the Organisation on several occasions to remove the photograph from its website, but to no avail.

3 At the Complainant's request, the Organisation subsequently removed the photograph from the website.

## ISSUE

4 The two main issues are (a) whether the Organisation breached its Consent Obligation[1] by failing to obtain the consent of the Complainant before disclosing his personal data and (b) whether any exceptions under the Personal Data Protection Act 2012[2] ("PDPA") in the Fourth Schedule

1 Pursuant to s 13 of the Personal Data Protection Act 2012 (Act 26 of 2012).
2 Act 26 of 2012.

applied. One such exception is where the personal data are publicly available.[3]

## FINDINGS

5 Investigations showed that the Organisation had collected the personal data of the Complainant, his father and a third family member, *ie*, their images, by taking a photograph of them in a public car park outside the premises of the Organisation's office, for which the Complainant agreed to pose. As the car park was an open area that was accessible to the public, the personal data in question could easily have been observed by reasonable means by members of the public at the material time.

6 As such, the circumstances under which the Respondent had collected, used and disclosed the personal data satisfies the publicly available exception under the PDPA.

7 Accordingly, since the publicly available exception was applicable, the Deputy Commissioner found that the Organisation was not in breach of the Consent Obligation by publishing the photograph on its website.

8 Following the above, given that the Organisation did not need to obtain consent from the Complainant in the first place, it was not obliged to respond to the Complainant's subsequent withdrawal of consent.

---

3 Personal Data Protection Act 2012 (Act 26 of 2012) Fourth Schedule, para 1(*d*).

Case Summary

# RE MY DIGITAL LOCK PTE LTD

***Consent Obligation*** *– Disclosure of personal data without consent in response to allegations by complainant – Disclosure was closely related to underlying dispute between parties*

22 December 2016

## BACKGROUND

1 This is the second complaint in an ongoing dispute between the Complainant and the Organisation. The outcome of the first complaint is set out in the decision of *Re My Digital Lock Pte Ltd* on 4 November 2016.[1] The outcome of the third complaint is set out in the decision of *Re My Digital Lock Pte Ltd* on 12 February 2018.[2]

2 As part of the ongoing dispute, the sole director ("Sole Director") of the Organisation set up a personal blog ("Blog") with the intent to respond to the various negative allegations made by the Complainant about the Organisation's business and the Sole Director. The Blog contained images and screenshots of the allegations that had been made by the Complainant on various websites and online forums, with the Sole Director's personal response appended to each of these allegations. The Blog was accessible to the public without any restrictions.

3 One of the screenshots posted on the Blog was a letter sent by the Organisation's solicitors to the Complainant. The screenshot was of an open window, which displayed a letter and the file name of the document in the title bar of the open window. The Complainant's name formed part of the file name of the document. Upon discovery, the Complainant filed a complaint to the Personal Data Protection Commission ("PDPC") on 9 September 2016.

---

1 [2017] PDP Digest 146.

2 [2018] PDP Digest 334.

## ISSUE

4 The issue is whether the Organisation was in breach of the Consent Obligation[3] by failing to obtain the consent of the Complainant before disclosing his personal data on the Blog.

## FINDINGS

5 *Prima facie*, the Organisation may have been in breach of the Consent Obligation as the Sole Director had disclosed the Complainant's personal data without consent by posting the screenshot of the letter which contained the Complainant's name. However, it was clear that the Sole Director's main intention in setting up the Blog was to respond to the Complainant's allegations, and not to disclose the identity of the Complainant. This was evidenced by the fact that although the Complainant's name was visible as part of the file name of the document, the Sole Director had taken care to redact the name and residential address of the Complainant in the body of the letter.

6 In the circumstances, the Deputy Commissioner was of the view that investigations should be discontinued, and the Organisation issued an Advisory Notice, for the following reasons:

> (a) the current complaint was closely tied to the ongoing defamation suit between the Organisation and the Complainant, and it was prudent for the PDPC to avoid a situation where its investigations into or findings concerning the legality or appropriateness of the disclosure of personal data on the Blog would influence the outcome of the ongoing legal proceedings, or inadvertently give leverage to one of the parties in the dispute;
> (b) it was not apropos for the PDPC to allow itself to be used by individuals as a tool in any private dispute, especially where the crux of the matter is not related to the protection of personal data; and

3 Pursuant to s 13 of the Personal Data Protection Act 2012 (Act 26 of 2012).

(c) the data protection dispute between the Complainant and the Organisation had essentially devolved into a private dispute between the Complainant and the Sole Director, as evidenced by the fact that the contents of the Blog mainly consisted of the Sole Director's personal rebuttal to the allegations made personally against him.

Case Summary

# RE SINGAPORE TELECOMMUNICATIONS LIMITED

***Investigations and Legal Proceedings*** *– Preservation of documents and evidence that may be material to investigation or court proceedings*
***Protection Obligation*** *– Unauthorised disclosure of customers' personal data to other customers – Software glitch in automated system*

11 April 2017

## BACKGROUND

1 The Organisation, a telecommunications company, relied on an automated process for its billing system. This automated system was designed to generate (a) bills of its subscribers ("Bill Run"), and (b) notification e-mails to its subscribers.

2 On 8 February 2016, the Complainant received an erroneous notification e-mail containing the personal data of another subscriber instead of his own. The personal data included the other subscriber's name, bill date, amount payable, due date for payment, account number and mode of payment.

3 The Commission's investigations discovered that due to a software glitch in the Organisation's internal job scheduling process, erroneous information was reflected in approximately 5,359 e-mail notifications.

4 On or about 8 February 2016, one Bill Run and two separate sets of notification e-mails were to be generated by the system. The Bill Run took a long time to be completed due to a subscriber account with an extraordinarily large bill. This in turn resulted in a delay in the generation of the first set of notification e-mails ("first job)", which only commenced at 7.34pm instead of the usual 11.00am. As the generation of the second set of notification e-mails ("second job") was scheduled to run at its usual time of 7.23pm, this resulted in the first job and second job running concurrently with an overlapping period of approximately 26 minutes. In view of the fact that both jobs used the same temporary output file during

the overlapping period, each job overwrote the output of the other, causing the e-mail contents to be mismatched and sent.

5 The Organisation voluntarily notified the Personal Data Protection Commission of the data leak incident on 11 February 2016.

## ISSUE

6 The issue is whether the Organisation was in breach of the Protection Obligation.[1]

## FINDINGS

7 The Organisation had deliberately set a buffer time of approximately seven hours between the first job and second job (*ie*, a start time of 11.00am for the first job and start time of 7.23pm for the second job) to avoid an overlap in the two jobs. The time taken for each of the runs were typically 30 to 50 minutes, much shorter than the allocated buffer time. The Organisation had been carrying out this process (with the same buffer time) for close to two years without incident.

8 Whilst the Organisation is obligated to put in place adequate pre-emptive measures to prevent overlapping jobs resulting in unintended data breaches, it would not be reasonable to impose on the Organisation an onerous responsibility of guarding against every single possibility of automated processes overlapping. The Commission is of the view that the Organisation took reasonable precautions to prevent overlapping of the two jobs by catering for the wide buffer time. Accordingly, the Commission found that there was no breach of the Protection Obligation.

## NEED FOR PARTIES TO PRESERVE ALL MATERIAL DOCUMENTS AND EVIDENCE

9 Notwithstanding the finding above, the Commission would provide some remarks relating to the investigation into this matter, and the need for parties to preserve all documents and evidence that may be material to the Commission's investigations.

---

1 Pursuant to section 24 of the Personal Data Protection Act 2012.

10 During the course of investigation, the Organisation was unable to provide the Commission with the relevant information and documents, such as the Bill Run log files, as the Organisation had the practice of retaining documents for a period of only three months before destroying them. In this case, the Organisation would have known or ought to have known that the circumstances pertaining to the Bill Run may be material to the investigation, given that in its notification to the Commission of the data breach on 11 February 2016 (just three days after the data breach incident), it was able to inform the Commission that the fault mainly lay with a particularly large Bill Run. Once the Organisation became aware that the circumstances surrounding the Bill Run may be a material fact or issue in the investigation, it ought to have taken steps to preserve the relevant information and documents as evidence.

11 Upon any party being aware that there may be information or documents that may be relevant to the Commission's investigations, it ought to take steps to preserve the relevant information or documents as evidence.

MCI (P) 035/07/2018